МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«МИРЭА – Российский технологический университет»

РТУ МИРЭА

Институт кибербезопасности и цифровых технологий

Кафедра КБ-2 «Информационно-аналитические системы кибербезопасности»

ДИСЦИПЛИНА	Основы информационной безопасности
	(полное наименование дисциплины без сокращений)
ИНСТИТУТ	Кибербезопасности и цифровых технологий
КАФЕДРА	«Информационно-аналитические системы кибербез-опасности»
	полное наименование кафедры)
ВИД УЧЕБНОГО	Лекция
МАТЕРИАЛА	(в соответствии с пп.1-11)
ПРЕПОДАВАТЕЛЬ	Шукенбаев А.Б.
	(фамилия, имя, отчество)
СЕМЕСТР	6
	(указать семестр обучения, учебный год)

Тема лекции: Введение в безопасность систем баз данных

1. Предмет дисциплины, структура и место курса в подготовке бакалавра.
2. Проблемы информационной безопасности баз данных.
3. Характеристики качества систем баз данных
4. Структура свойства информационной безопасности баз данных

Учебные и воспитательные цели:

1. Сформировать у обучающихся представление о предмете, изучаемом в рамках курса «Безопасность систем баз данных».

2. Способствовать формированию у обучающихся компетенций предусмотренных рабочей программой в соответствии с требованиями ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность направленности – «Безопасность автоматизированных систем».

3. Воспитать чувство ответственности за порученное дело, исполнительности, аккуратности, добросовестности, чувства долга, ответственности за сохранение тайны.

Время: 2 часа (90 мин.).

Литература:

Основная:

1. Зайцев А. П., Мещеряков Р. В., Шелупанов А. А. Технические средства и методы защиты информации [Электронный ресурс]: - Москва: Горячая линия-Телеком, 2018. - 442 с. – Режим доступа: https://e.lanbook.com/book/111057

2. Гулаков В. К., Трубаков А. О., Трубаков Е. О. Структуры и алгоритмы обработки многомерных данных [Электронный ресурс]: монография. - Санкт-Петербург: Лань, 2018. - 356 с. – Режим доступа: https://e.lanbook.com/book/107305

3. Душкин А. В., Барсуков О. М., Кравцов Е. В., Славнов К. В. Программно-аппаратные средства обеспечения информационной безопасности [Электронный ресурс]: - Москва: Горячая линия-Телеком, 2018. - 248 с. – Режим доступа: https://e.lanbook.com/book/111053

4. Казаков Ю. М., Тищенко А. А., Кузьменко А. А., Леонов Ю. А., Леонов Е. А. Методология и технология проектирования информационных систем [Электронный

ресурс]: учебное пособие. - Москва: ФЛИНТА, 2018. - 136 с. – Режим доступа: https://e.lanbook.com/book/113460

5. Жук А. П., Жук Е. П., Тимошкин А. И., и др. Защита информации: учебное пособие. - М.: РИО, 2018. - 400 с.

6. Остроух А. В., Суркова Н. Е. Проектирование информационных систем [Электронный ресурс]: монография. - Санкт-Петербург: Лань, 2019. - 164 с. – Режим доступа: https://e.lanbook.com/book/118650

7. Никифоров С. Н. Методы защиты информации. Защита от внешних вторжений [Электронный ресурс]: учебное пособие. - Санкт-Петербург: Лань, 2019. - 96 с. – Режим доступа: https://e.lanbook.com/book/114697

8. Магомедов Ш. Г. Методы и средства защиты информации: учебное пособие. - М.: МИРЭА, 2018. - 92 с.

9. Бондарев В.В. Введение в информационную безопасность автоматизированных систем [Электронный ресурс]: учебное пособие/ Бондарев В.В.— Электрон. текстовые данные. — Москва: Московский государственный технический университет имени Н.Э. Баумана, 2018. — 252 с.— Режим доступа: http://www.iprbookshop.ru/94747.html. — ЭБС «IPRbooks»

Дополнительная литература

1. Шелухин О. И., Сакалема Д. Ж., Филинова А. С. Обнаружение вторжений в компьютерные сети (сетевые аномалии) [Электронный ресурс]: - Москва: Горячая линия-Телеком, 2018. - 220 с. – Режим доступа: https://e.lanbook.com/book/111119

2. Малюк А. А., Горбатов В. С., Королев В. И., Фомичев В. М., Дураковский А. П., Кондратьева Т. А. Введение в информационную безопасность [Электронный ресурс]: - Москва: Горячая линия-Телеком, 2018. - 288 с. – Режим доступа: https://e.lanbook.com/book/111075

3. А. А. Агафонов, А. С. Юмаг. Безопасность систем баз данных: учеб. Пособие. М-во науки и высш. образования Рос. Федерации, Самар. нац. исслед. ун-т им. С. П. Королева (Самар. ун-т). - Самара: Изд-во Самар. ун-та, 2023. http://repo.ssau.ru/handle/Uchebnye-izdaniya/Bezopasn...

4. Пригонюк Н.Д., Петров В.И. Основы построения защищенных баз данных: Учебное пособие. — Воронеж: ООО «МИР», 2019. — 76 с

Учебно-материальное обеспечение:

1. Наглядные пособия.
2. Технические средства обучения: проектор.
3. Приложения: рисунки, таблицы, слайды.

ПЛАН ЛЕКЦИИ:

Введение – до 5 мин.

Основная часть (учебные вопросы) – до 80 мин.

1-й учебный вопрос: Предмет дисциплины, структура и место курса в подготовке бакалавра. – 15 мин.

2-й учебный вопрос: Проблемы информационной безопасности баз данных. – 25 мин.

3-й учебный вопрос: Характеристики качества систем баз данных. – 20 мин.

4-й учебный вопрос: Структура свойства информационной безопасности баз данных. – 20 мин.

Заключение – до 5 мин.

Введение – до 5 мин.

Методические рекомендации:

- показать актуальность темы;

- довести целевую установку через основные положения лекции;

- охарактеризовать место и значение данной темы в курсе;

- описать обстановку, в которой разрабатывалась теоретическая проблема и шла ее практическая реализация;

- дать обзор важнейших источников, монографий, литературы по теме;

- вскрыть особенности изучения обучающимися материала по рассматриваемой проблеме.

Основная часть – до 80 мин.

Дисциплина «Безопасность систем баз данных» имеет своей целью способствовать формированию у обучающихся профессиональных компетенций **ОПК-2.2,**

ОПК-12 в соответствии с требованиями ФГОС ВО по направлению 10.03.01 «Информационная безопасность».

Место дисциплины в структуре основной образовательной программы:

Для освоения дисциплины «Безопасность систем баз данных» обучающиеся должны обладать знаниями, умениями и навыками, полученными в результате формирования и развития компетенций в предыдущих дисциплинах и практиках.

Главной задачей курса является формирование у обучающихся специализированной базы знаний по основным понятиям и направлениям в области разработки и проектирования безопасности систем баз данных, технологий, методов, концепций и инструментальных средств для их реализации.

Мы приступаем к изучению дисциплины «Безопасность систем баз данных». Она является одной из основных при изучении курса дисциплин по разработке и проектированию защищенных автоматизированных информационных систем. Знания и практические навыки, полученные из курса «Безопасность систем баз данных», используются при изучении других научных дисциплин, а также при выполнении курсовых и выпускных квалификационных работ. Изучаться дисциплина будет в течении семестра.

1.2 Проблемы информационной безопасности баз данных (БД)

База данных *- это поименованная совокупность взаимосвязанных данных, находящихся под управлением СУБД*

СУБД *– программный комплекс поддержки интегрированной совокупности данных, предназначенный для создания, ведения и использования базы данных многими пользователями (прикладными программами).*

Основные функции СУБД

1. Непосредственное управление данными во внешней памяти

2. Управление буферами оперативной памяти

3. Управление транзакциями

4. Журнализация

5. Поддержка языков БД

Информационная система *— взаимосвязанная совокупность средств, методов и персонала, используемых для хранения, обработки и выдачи информации в интересах достижения поставленной цели.*

Безопасность баз данных» (Database security) относится к использованию широкого спектра средств защиты информации для защиты баз данных (потенциально включая данные, приложения баз данных или хранимые функции, системы баз данных, серверы баз данных и связанные с ними сетевые ссылки) против компрометации их конфиденциальности, целостности и доступности. Он включает в себя различные типы или категории контроля, такие как технические, процедурные /административные и физические.

Безопасность баз данных – состояние защищенности баз данных (БД), приложений БД или хранимых функций, серверов БД и связанных с ними сетевых ссылок, достигаемое за счет использования широкого спектра средств защиты данных.

Проблема обеспечения безопасности данных появилась в ходе расширения круга пользователей вычислительных систем. Рост числа ЭВМ и сфер их использования расширил возможности модификации, хищения и уничтожения данных. Еще более усугубило проблему обеспечения безопасности данных появление автоматизированных информационных систем (АИС). Атаки на БД и хранилища являются очень опасными для организаций. В последние годы число утечек растёт, причём не менее 30 % нарушений целостности данных связно с внешним вмешательством. Как правило, киберпреступников чаще всего интересуют персональные данные сотрудников, информация о клиентах и заказчиках, результаты исследований рынка, финансовая и платёжная информация, анализ деятельности конкурентов и другие сведения, которые практически всегда есть в корпоративных базах данных.

Ввиду особой значимости и ценности такой информации, возникает необходимость в повышении безопасности как элементов инфраструктуры, так и, собственно, самих баз данных (БД).

Сегодня практически все крупнейшие производители СУБД развивают концепцию конфиденциальности и целостности данных при их доступности. Дей-

ствия крупных игроков рынка направлены, прежде всего, на преодоление уже известных уязвимостей, рассмотрение вопросов, специфичных для определённой системы управления базами данных, реализацию основных моделей доступа к БД. Но этот подход способен решать лишь конкретные задачи, однако **общей концепции безопасности для СУБД не существует**. Такое положение вещей не может не усложнять задачи обеспечения безопасности баз данных на предприятии.

Взгляд в прошлое: история развития СУБД с эволюционной точки зрения

Исторически сложилось так, что системы безопасности баз данных развивались в качестве реакции на действия киберпреступников. Оказало влияние и общее развитие баз данных, начиная с решений на мейнфреймах, заканчивая облачными хранилищами.

Специалисты выделяют следующие **архитектурные подходы**:

— полный доступ пользователей к серверу баз данных;

— внедрение системы аудита (логов действий юзеров) средствами СУБД;

— деление пользователей на частично доверенных и доверенных с помощью средств СУБД;

— внедрение шифрования данных с выносом средств аутентификации за пределы СУБД в промежуточное программное обеспечение и операционные системы;

— исключение полностью доверенного администратора данных.

Внедрение средств защиты, разумеется, необходимо. Но если это происходит лишь как реакция на угрозу, защита от новых способов атак не обеспечивается, да и вообще, о проблеме безопасности баз данных формируется весьма разрозненное представление.

Также существует множество разнородных средств повышения безопасности БД, что стало причиной отсутствия понимания комплексной безопасности баз данных. Нет общего подхода и к обеспечению безопасности хранилищ данных. Сложно спрогнозировать атаки, разработать действенные защитные механизмы.

Мало того, многие системы не защищены от уже давно известных атак, а подготовка специалистов не отлажена.

Проблемы безопасности БД

Киберпреступность развивается одновременно с базами данных и средствами защиты. Но, несмотря на это, за последние годы список главных уязвимостей СУБД мало изменился. Выполнив анализ архитектуры БД, известных уязвимостей, имеющихся средств обеспечения безопасности СУБД и прецедентов нарушения безопасности, можно отметить следующие причины появления проблем:

— разработчики баз данных, администраторы и программисты уделяют недостаточное внимание вопросам безопасности баз;

— разные СУБД применяют различные языковые конструкции доступа к данным, однако они организованы на основе той же модели;

— всерьёз занимаются проблемами безопасности лишь крупные производители СУБД (DB2 Universal Database и Informix Dynamic Server (IBM), Oracle9i (Oracle), SQL Server (Microsoft), Adaptive Server Enterprise и Adaptive Server IQ (Sybase));

— возникают новые модели хранения данных и их виды, сразу попадая в зону риска.

Кроме того, ряд уязвимостей потенциально опасны из-за банального **невнимания**, а иногда даже и незнания администраторами систем БД вопросов безопасности. К примеру, широко эксплуатируются в отношении веб-приложений простые SQL-инъекции, в которых достаточное внимание входным данным запросов не уделено.

Внедрение SQL-кода (SQL –ingiectio) – один из самых распространенных способов взлома сайтов и программ, работающих с БД основанный на внедрении в запрос произвольного SQL кода

Для предприятий финансовым компромиссом является использование разных средств обеспечения информационной защиты, ведь внедрение продуктов повышенной защищённости и подбор высококвалифицированного персонала — это

очень большие затраты. Однако стоит понимать, что компоненты безопасности могут оказывать на производительность СУБД негативное влияние.

Проблема усугубляется и широким распространением **нереляционных СУБД** — они оперируют другой моделью данных, но построены по тем же принципам, если сравнивать с реляционными. Нельзя не вспомнить и про многообразие современных NoSQL-решений — это становится причиной разнообразия используемых моделей данных, и, в свою очередь, размывает границу понятия БД в целом.

Следствие вышеперечисленных проблем — это отсутствие единых методик защиты баз. Если говорить о NoSQL-системах, то тут отсутствуют не только общепринятые механизмы сохранения целостности (например, шифрование и аудит данных), но и развитые средства для аутентификации пользователей.

Каковы особенности защиты БД?

Современные хранилища данных состоят из двух компонентов: хранимых данных (собственно, БД) и программ для управления (СУБД).

Обеспечить безопасность нельзя, не организовав безопасное управление данными. А значит, все уязвимости и вопросы защиты СУБД можно поделить на 2 категории: *независящие и зависящие от данных*.

Те уязвимости, которые от данных не зависят, характерны и для других видов программного обеспечения. Причина проблем тут разная — это и несвоевременное обновление, и недостаточная квалификация админа, и наличие неиспользуемых функций.

Однако практика показывает, что большая часть аспектов безопасности СУБД как раз-таки зависит от данных. К примеру, многие СУБД поддерживают запросы через некоторый язык, содержащий наборы функций, доступных пользователю. А архитектура используемых языков связана с моделью данных, которая применяется для хранения информации. В результате можно сказать, что модель отчасти определяет особенности языка, а особенности языка определяют наличие в нём определённых уязвимостей. При этом такие общие уязвимости, допустим,

как инъекции, выполняются по-разному (Java-инъекция, SQL-инъекция) с учётом синтаксиса языка.

Основные требования к безопасности БД

Выше уязвимости мы разделили (независящие и зависящие от данных). Теперь выделим независящие и зависящие от данных меры по обеспечению безопасности хранилищ.

Требования по безопасности к системе БД, не зависящей от данных:

1. **Работа в доверенной среде**. Доверенная среда — инфраструктура предприятия с её защитными механизмами, обусловленными политикой безопасности.

2. **Обеспечение физической безопасности файлов данных**. Здесь требования не отличаются от тех, которые применимы к любым другим файлам приложений и пользователей.

Требования к целостности информации для систем, зависящим от данных:

1. **Безопасность пользовательского программного обеспечения**. Речь идёт о задачах построения безопасных механизмов доступа и интерфейсов.

2. **Безопасная организация работы с данными**. Организация данных и управление ими — ключевой вопрос для системы хранения информации. Сюда входит и задача по организации данных с контролем целостности, и другие задачи, порой специфичные для СУБД.

Аспекты создания защищённых БД

Чтобы решить обозначенные проблемы и обеспечить информационную безопасность СУБД, надо перейти от практики закрытия уязвимостей к **комплексному подходу**, призванному обеспечить более эффективную безопасность хранилищ данных. Вот основные этапы перехода к этому:

1. **Разработка комплексных методик**, обеспечивающих безопасность хранилищ данных. Комплексные методики применяются как при разработке, так и при внедрении хранилищ данных и программного обеспечения. Следование такому подходу избавит от множества ошибок управления СУБД, поможет защитить данные от распространённых уязвимостей.

2. **Оценка и классификация угроз СУБД**. После классификации появляется возможность упорядочить угрозы и уязвимости с целью последующего анализа и обеспечения защиты. Специалисты по безопасности установят зависимость между проблемами и причинами их возникновения. Таким образом, после введения конкретного механизма в СУБД, администраторы и разработчики смогут спрогнозировать связанные с новым механизмом угрозы, а значит, заранее подготовят соответствующие средства по обеспечению безопасности.

3. **Разработка стандартизированных механизмов** обеспечения безопасности. В случае стандартизации языков работы с данными и подходов к защите появляется возможность создания средств безопасности, применимых к разным СУБД. На момент написания материала, к сожалению, речь идёт лишь о методических и теоретических средствах, так как появление уже готовых комплексных программных средств зависит лишь от разработчиков СУБД и производителей, точнее, от их желания следовать стандартам.

Выделяются следующие основные **этапы развития концепций обеспечения безопасности данных**.

Этап 1. Основная идея этапа – обеспечение ИБ механизмами, которые функционируют по строго формальным алгоритмам. В целях создания таких механизмов использовались технические и программные средства. При этом программные средства ЗИ включались в состав операционных систем (ОС) и систем управления базами данных (СУБД).

Недостатком разработанных подходов к ЗИ была технология разграничения доступа пользователей к данным. В связи с этим, для повышения эффективности ЗИ, был использован дифференцированный доступ к данным. Однако испытания ряда систем (ADEPT-50, MULTICS), показали, что такого рода системы, с точки зрения обеспечения ИБ, имеют множество недостатков. Усложнение программных систем (ПС) и увеличение числа пользователей АИС обусловило потребность в разработке идей ЗИ на более высоком уровне абстракции.

Этап 2. Главное достижение этого этапа – разработка концепции и реализации специального программного компонента, управляющего программными и, частично,

аппаратными средствами ЗИ – ядра безопасности.

В составе ОС ядро безопасности реализовывалось как функционально самостоятельная подсистема управления механизмами ЗИ, которая включала технические, программные, и лингвистические средства. Концепции ЗИ в СУБД в основном состояли из модификаций соответствующих разработок для ОС.

По мере совершенствования методологий построения моделей данных и языка SQL стало понятно, что проблема обеспечения безопасности БД имеет специфические особенности, в первую очередь относящиеся к области информационного и лингвистического обеспечения.

В ходе осознания роли собственника информации улучшались механизмы ЗИ, которыми могли бы управлять пользователи АИС. Однако, несмотря на принимаемые меры, обеспечение эффективной ЗИ обеспечить не удалось, о чем говорят множественные факты нарушения ИБ.

Этап 3. Проблема обеспечения ИБ трансформировалась от описательного до научного уровня осмысления. Особенностью третьего этапа является применение принципа системности, в соответствии с которым обеспечение ИБ представляется как регулярный процесс, затрагивающий все этапы жизненного цикла (ЖЦ) АИС при комплексном использовании всех средств и механизмов ЗИ.

При этом все средства и механизмы, применяемые в целях ЗИ, объединяются в систему обеспечения ИБ, которая должна обеспечивать многоуровневую ЗИ не только от злоумышленников, но и от обслуживающего персонала АИС, а также от случайных ошибок пользователей.

Начало этим процессам было положено исследованиями вопросов ЗИ, проведенными в начале 80-х годов Национальным центром компьютерной безопасности NCSC (National Computer Security Center).

Результат этих исследований – изданный министерством обороны США (1983 г.) документ под названием «Критерии оценки надежных компьютерных систем». Впоследствии, по цвету обложки, документ получил название «Оранжевая книга».

Этот документ может считаться первым стандартом в области создания защищенных компьютерных систем (КС), ставшим впоследствии основой организации

системы сертификации КС по критериям ЗИ. Подходы к построению и анализу защищенных систем, представленные в «Оранжевой книге», послужили методологической и методической базой для дальнейших исследований в этой сфере.

В 1991 г. NCSC был опубликована Интерпретация «Критериев оценки надежных компьютерных систем» в применении к понятию надежной СУБД. Этот документ, конкретизирующий и развивающий положения «Оранжевой книги» для решения задачи создания и оценки защищенных СУБД, известен также как «Розовая книга».

Аналогичные исследования по проблемам компьютерной безопасности были проведены во многих странах и созданы соответствующие национальные стандарты в этой сфере.

В России ФСТЭК (Гостехкомиссией при Президенте РФ) были разработаны и в 1992 г. опубликованы «Руководящие документы по защите от несанкционированного доступа к информации». В документах определяются требования, методика и стандарты построения защищенных средств ВТ и ПО (для этих целей определен 21 показатель).

Во всех перечисленных выше документах уровень безопасности средств ВТ или ПО характеризуется принадлежностью к одному из иерархически упорядоченных классов.

Так «Руководящие документы по защите от несанкционированного доступа к информации» определяют семь классов (самый низкий класс – седьмой, самый высокий – первый).

Иерархическая упорядоченность классов защищенности подразумевает, что если наличие некоторого средства ЗИ от несанкционированного доступа требуется для ВТ или ПО определенного класса, то это же средство потребуется и для средства ВТ более высокого класса. Существо требований к оцениваемой системе может только усиливаться при переходе к более высоким классам защищенности.

По защищенности процессов обработки информации все АИС делятся на три группы.

Третья группа включает в себя АИС, 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 АИС, в которых информация обрабатывается и хранится на носителях различного уровня конфиденциальности. Если пользователь имеет одинаковые права доступа ко всей обрабатываемой и хранимой информации, то АИС относится ко второй группе. В тех же случаях, когда не все пользователи имеют права доступа ко всей информации, АИС относится к первой группе.

Комплекс организационных и программно-технических средств мер по ЗИ от несанкционированного доступа предусматривает наличие:

— подсистемы управления доступом;

— подсистемы регистрации и учета;

— криптографической подсистемы;

— подсистемы обеспечения целостности.

Процесс аттестации конкретной АИС состоит в проведении экспертизы с целью отнесения АИС к определенному классу. Процесс экспертизы состоит из формальной проверки наличия свойств, перечень которых определен в соответствующем руководящем документе (стандарте):

- приказе ФСТЭК №77 от 29 апреля 2021 года.
- постановлением Правительства РФ №676 от 6 июля 2015 года,
- требования к защите информации в таких системах определены в приказе ФСТЭК России №17 от 11 февраля 2013 года,
- требования к сертификации средств защиты прописаны в другом приказе регулятора, №55 от 3 апреля 2018 года.

Накопленный опыт в области обеспечения ИБ, развитие теории ИБ стали объективной основой стандартизации в данной сфере.

Этап 3. Характеризуется разработкой и внедрением стандартов в области ИБ. На этом этапе решается задача управления обеспечением ИБ конкретного объекта, например, базы данных. Цель такого управления – обеспечение требуемого уровня

ЗИ активов от объективно существующих угроз. Требуемый уровень ЗИ определяется как разумный баланс между потенциальным ущербом, связанным с реализациями существующих угроз, и затратами на обеспечение процесса управления.

Представителями государственных организаций европейских стран, США, Канады и др. были развернуты работы по созданию международного стандарта в области оценки безопасности ИТ. Работа по созданию нового стандарта координировалась **Международной организации по стандартизации** (**ISO**) и была направлена, в первую очередь, на унификацию (гармонизацию) национальных стандартов в области оценки ИБ и повышение уровня доверия к оценке безопасности ИТ.

Стандарт получил название **ISO/IEC 15408** и стал известен как «Общие критерии». Его принятие отразило изменения, происходящие в идеологии подхода к построению безопасных ИТ, в частности, защищенных ИС и их программного ядра – СУБД.

В отличие от «Оранжевой книги» и руководящих документов Гостехкомиссии в новом стандарте ***отсутствует фиксированный набор классов защищенности***. Основная идея «Общих критериев» состоит в разделении всех требований безопасности на две категории:

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

В 2002 г. на основе аутентичного текста ISO/IEC 15408 был принят российский стандарт **ГОСТ Р ИСО/МЭК 15408-2-2013 «**Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий»

Близкий подход к анализу защищенности ИС был предложен в британском стандарте **BS 7799** «Практические правила управления информационной безопасностью». Содержательное существо стандарта состоит в обобщении опыта обеспечения ИБ ИС различного назначения.

Стандарт **BS 7799** послужил основой для разработки стандарта **ISO 17799** Информационная технология. Практические правила управления информационной безопасностью. Базис стандарта состоит в определении и оценке уязвимых мест в анализируемой ИС, оценке уровня существующих угроз и определения комплекса мер, позволяющего снизить риски до приемлемого для организации уровня. Выбор комплекса осуществляется на основе стоимостного анализа потенциальных потерь, связанных с реализацией конкретных угроз. Стандарт содержит практические правила обеспечения ИБ ИС для всех этапов ЖЦ 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.

Соблюдение предписанных технологий обеспечения ИБ гарантирует некоторый базовый уровень ИБ ИС. В случае повышенных требований к ИБ ИС производится оценка ценности ресурсов, характеристик информационных рисков и уязвимости системы, на основе которых осуществляется выбор системы защиты информационных ресурсов.

1.2. Характеристики качества систем баз данных

Современные БД являются одними из массовых специфических объектов в сфере информатизации, для которых в ряде областей необходимо особенно высокое качество и квалифицированное системное проектирование. При выполнении анализа безопасности систем баз данных (СБД) целесообразно рассматривать два аспекта:

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

Поэтому и при анализе качества СБД выделяют два основных компонента, представленных на рисунке 1:

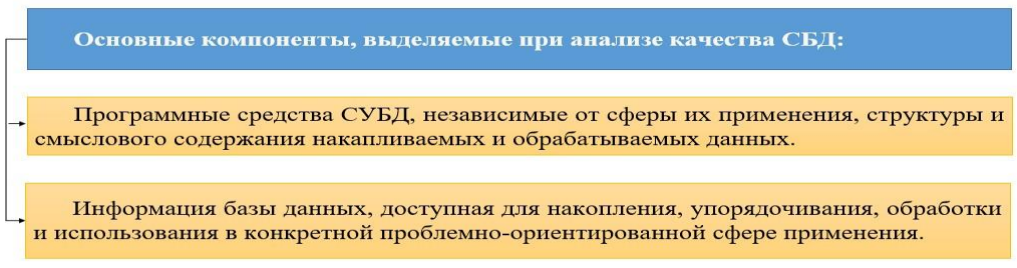


Рис. 1 – Основные компоненты, выделяемые при анализе качества СБД

Первый компонент – это комплекс программ СУБД. При формировании требований к качеству СУБД может быть использован практически весь набор атрибутов и характеристик качества программных систем, описанный в стандарте **ISO 9126**. При упорядочении и выборе этих показателей есть особенности, состоящие в адаптации и изменении акцентов. В любом из случаев наиболее значимые характеристики качества СУБД – это требования к функциональной пригодности для процессов создания и модификации информационного наполнения БД системными администраторами, а также доступа к данным и представления результатов пользователям БД.

Оценка качества интерфейса специалистов с БД, обеспечиваемого средствами СУБД, во многом является субъективной. При этом имеется ряд характеристик, оценка которых может быть выполнена достаточно корректно.

В зависимости от предметной области применения СУБД, приоритет в ходе системного анализа требований к качеству систем БД может быть отдан различным конструктивным характеристикам, представленными на рис. 2.

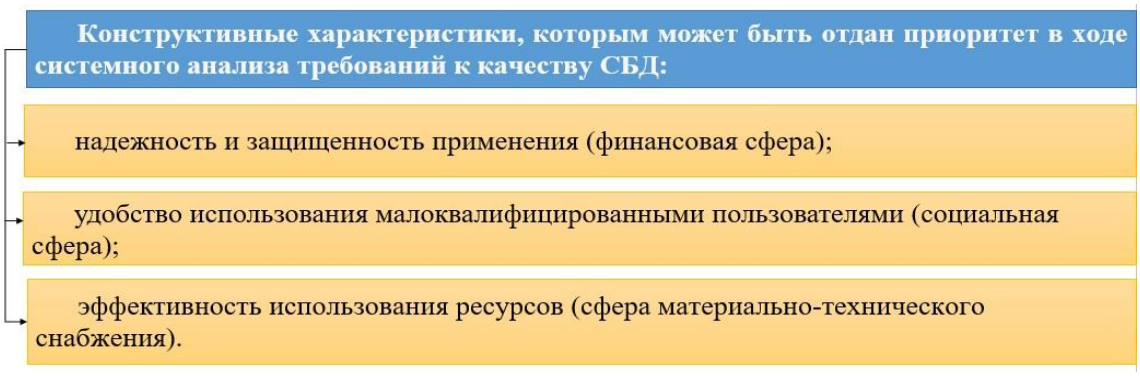


Рис. 2 – Приоритетные конструктивные характеристики, которым может быть отдан приоритет

При этом практически во всех случаях сохраняется некоторая роль ряда других конструктивных показателей качества. Для каждого из них необходимо анализировать и определять его приоритет для конкретной сферы применения, меры и шкалы необходимых и допустимых характеристик качества.

Второй компонент БД – это непосредственно накапливаемая и обрабатываемая информация. В СБД превалирующее значение отдается самим данным, их хранению и технологии обработки.

Используемые требования и показатели качества должны иметь практическую значимость как для владельцев информационных ресурсов (ИР), так и для пользователей. Кроме того, каждый выделяемый показатель качества СБД должен быть пригодным для выполнения достоверной оценки или для измерения, а также для сравнения с нужным значением, указанным в ТЗ на проектирование системы.

Характеристики качества СБД делятся на функциональные и конструктивные.

Функциональная пригодность СБД в процессе проектирования находится исходя из требований к реальным значениям показателей и критериям качества. Наиболее сложной такая задача является для больших (big data) и распределенных БД, связанных с обработкой многоаспектной информации об исследуемых объектах. В качестве меры качества функциональной пригодности может быть использована степень соответствия доступной пользователям информации целям и назначению СБД.

Big Data — это крупные массивы разнообразной информации и стек специальных технологий для работы с ней. Термин применяется к таким объемам данных, с которыми пользовательский компьютер и офисные программы не справятся.

Функциональная пригодность СБД представляется характеристиками, изображенными на рис. 3.

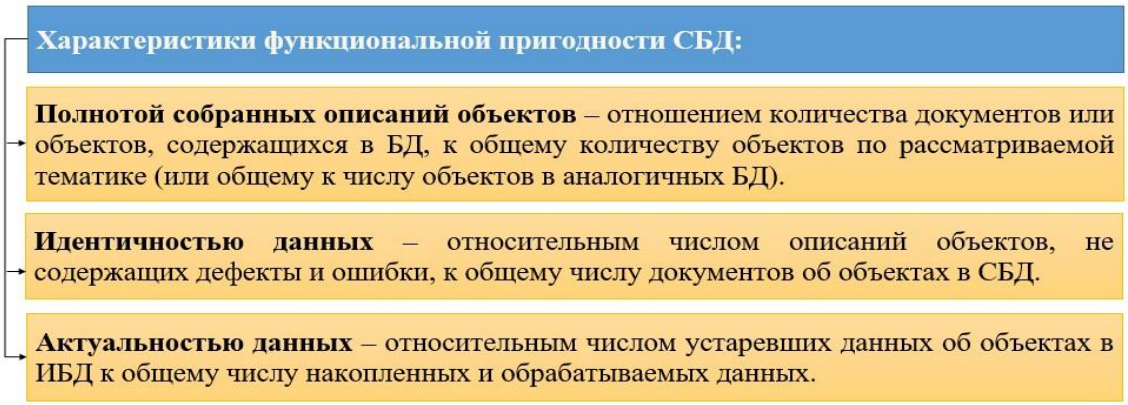


Рис. 3 – Характеристики функциональной пригодности СБД

К *конструктивным характеристикам* качества информации СБД могут быть отнесены практически все показатели качества ПС, описанных в стандарте ISO 9126.

Требования к информации БД также должны содержать особенности обеспечения ее достоверности, надежности, актуальности, эффективности использования вы-

числительных ресурсов и приемлемого уровня сопровождения. Содержание и сущность этих конструктивных характеристик как базовых понятий и характеристик качества СБД нужно применять в процессе проектирования ИС. Для оценивания конструктивных характеристик могут применяться те же меры и шкалы, что и при анализе качества ПС.

Выделяются характеристики защищенности информации и достоверности данных.

Достоверность данных – это степень соответствия информации об объектах в СБД моделируемым реальным объектам в рассматриваемый момент времени. В качестве причин нарушения достоверности данных могут выступать изменения самих объектов, которые некорректно или несвоевременно отображаются в их образах в БД. При проектировании выбор и разработка требований к достоверности БД могут быть оценены по степени покрытия достоверными данными состояния и изменения внешних объектов, которые они отражают.

В качестве значимых показателей качества БД также выступают объемновременные характеристики (рисунок 4):

— объем БД – относительное число записей описаний объектов (или документов) в БД, доступных для хранения и обработки, в сравнении с полным количеством 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 БД;

— глубина ретроспективы – максимальный интервал времени от даты выпуска и/или записи в БД 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.

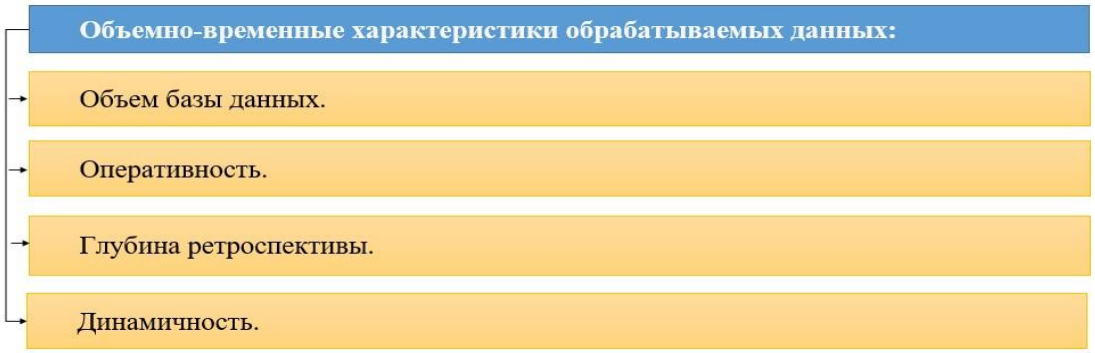


Рис. 4 – Объемно-временные характеристики обрабатываемых данных

Отдельно отметим такую характеристику как *защищенность информации* БД, которая реализуется, в основном, программными средствами СУБД, однако в сочетании с поддерживающими их средствами организации и защиты данных. Цели, назначение и функции защиты тесно связаны с особенностями функциональной пригодности каждой ИБД. При системном проектировании свойства защищать информацию баз данных от негативных воздействий описываются обычно составом и номенклатурой методов и средств, используемых для защиты от внешних и внутренних угроз. Косвенным показателем ее качества может служить относительная доля вычислительных ресурсов, используемых непосредственно средствами защиты информации БД.

Основное внимание в практике обеспечения безопасности применения БД сосредоточено 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. 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 можно характеризовать величиной потенциального ущерба, риск возникновения которого при проявлении дестабилизирующих факторов и реализации конкретных угроз безопасности удается предотвратить или понизить. Также возможной характеристикой качества может выступать среднее время между возможными проявлениями угроз, преодолевающих защиту данных.

1.3 Структура свойства информационной безопасности баз данных

В качестве основного элемента современных АИС выступает СУБД. При работе пользователь на доступном ему языке выполняет формулировку своих информационных потребностей. При этом требуется некоторая компонента системы обработки информации, обеспечивающая взаимодействие с пользователем на понятном ему языке. Это связано с тем, что существующие технические средства (ТС) могут воспринимать только язык детальных инструкций.

Кроме того, необходимы ТС, которые бы обеспечивали удовлетворяющий проектировщиков и разработчиков системы языковый уровень описания технологических процессов обработки данных. Две эти задачи решаются с использованием средств СУБД.

Для существующего в настоящее временя уровня развития распределенной обработки данных характерно размещение логически единой информационной базы в распределенной сетевой среде с организацией разграничения доступа. При этом имеющиеся трудности в области управления доступом должны быть скрыты от пользователя. Логическое пространство БД должно восприниматься пользователя как единое, как бы располагаемое на его локальной рабочей станции.

Удовлетворяющая степень ИБ СБД должна обеспечиваться без снижения функциональных характеристик АИС и без усложнения условий работы пользователя с АИС. Способы обеспечения ИБ БСД должны обладать удобством администрирования СБД и АИС в целом и гибкостью.

Обеспечение ИБ СБД связано с необходимостью разработки методов и реализующих их инструментальных средств, которые бы обеспечили реализацию трех взаимозависимых свойств СБД, представленных на рис. 5.

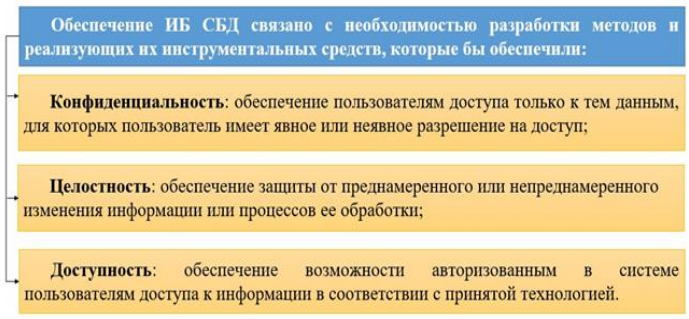
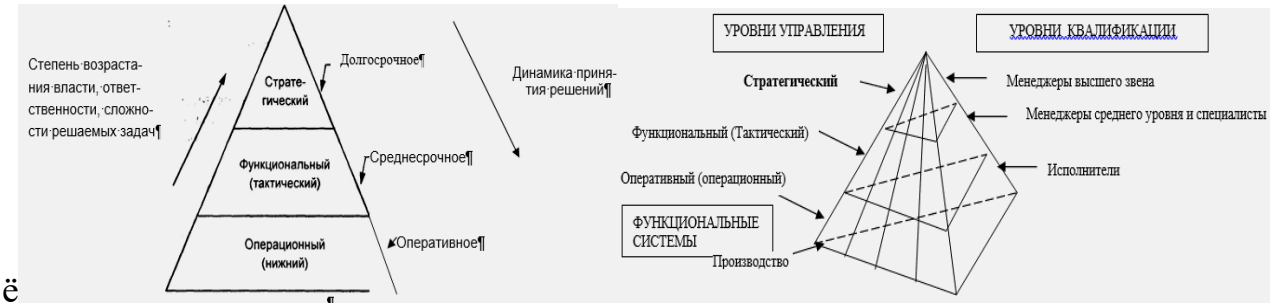


Рис. 5 – Взаимосвязанные свойства СБД

Методы и инструментальные средства выполнения задач, обеспечивающих решение трех указанных взаимосвязанных свойств (с учетом существующих ограничений по используемому ресурсному обеспечению) являются характерными для любых СБД.

Так, для систем организационного управления и информационного обеспечения процесса принятия решений задача обеспечения секретности предусматривает комплекс мер по предотвращению НСД к *конфиденциальной информации* какими-либо пользователями. 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. При этом обычно предполагается, что используемые правила обеспечивают однозначное решение о разрешении или запрещении доступа к данным.

Задача *обеспечения целостности* предусматривает комплекс мер по предотвращению непреднамеренного изменения или уничтожения информации, используемой ИСУ или СППР. 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.



ё

Рис. 6. Пирамида уровней управления, отражающая возрастание власти, ответственности, сложности и динамику принятия решений/

Системы обработки данных (СОД) предназначены для учета и оперативного регулирования хозяйственных операций, подготовки стандартных документов для внешней среды (счетов, накладных, платежных поручений).

***Информационные системы управления (ИСУ*)** ориентированы на тактический уровень управления: среднесрочное планирование, анализ и организацию работ в течение нескольких недель (месяцев), например анализ и планирование поставок, сбыта, составление производственных программ.

***Системы поддержки принятия решений (СППР*)** используются в основном на верхнем уровне управления (руководства фирм, предприятий, организаций), имеющего стратегическое долгосрочное значение в течение года или нескольких лет.

Задача *обеспечения доступности информации* предусматривает систему мер по поддержке всем легитимным пользователям доступа к ресурсам системы в соответствии с принятой технологией (например, круглосуточно). Причиной отказа в доступе может быть перегрузка системы, вы званная потоком «информационного шума» (спам, искусственно формируемый поток бессмысленных запросов), перегрузка системы, вызванная объективными причинами (резкое увеличение потока запросов в связи с некоторыми событиями), действия, направленные на остановку критически важных процессов (например, компонент сервера БД, прослушивающего процесса). Структура свойства ИБ представлена на рис. 7.

Рис. 7 – Структура свойства ИБ

Необходимой частью любой защищенной АИС является функция регистрации раз личных событий (действий) в системе – аудит. Постепенно в среде руководителей, отвечающих за информационное обеспечение конкретных систем, растет понимание того, что гарантированно защищенных серверов БД нет, и их создание в ближайшие годы не предвидится.

Этот факт объясняется сложностью и многофункциональностью объектов информатизации. При этом важно иметь в виду не только сложность программной и аппаратной реализации АИС, но и сложность адекватного алгоритмического описания процессов обработки, хранения и передачи информации в современных системах

обработки данных.

Нет абсолютно надежных средств защиты сред ы 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 БД.

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

СУБД является сложным, многокомпонентным, распределенным программным комплексом. Архитектура построения СУБД, логика представления информации предмет ной области базами данных в процессе длительной эволюции также стали достаточно сложными, а иногда и запутанны ми. С каждой новой версией СУБД увеличивается число управляемых параметров системы, в том числе и параметров, определяющих характеристики ИБ. Естественным методом борьбы со сложностью изучаем ой системы является ее структуризация. Поэтому в данной лекции и методы обеспечения информационной безопасности баз данных будут рассматриваться как совокупность методов и средств обеспечения конфиденциальности, целостности и доступности.

Первым этапом анализа уровня ИБ СБД должен быть этап выявления угроз. Угрозы ИБ всегда объективно существуют при использовании информационных технологий. Источники угроз определяются средой, в которой происходит работа с БД, и субъекты, осуществляющие обработку информации. Определение субъектов информационных отношений на уровне предметной области и выявление интересов этих субъектов – необходимые предпосылки для профессионального проведения анализа ИБ СБД.