Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056:004.6

Конопелько
Илья Александрович

# Обеспечение безопасности систем управления реляционными базами данных

**АВТОРЕФЕРАТ**
на соискание степени магистра технических наук

по специальности 1-988001 Методы и системы защиты информации, информационная безопасность

Научный руководитель

Ширинский Валерий Павлович

Кандидат технических наук,
Доцент

Минск 2018

# ВВЕДЕНИЕ

Безопасность информационных систем является частью более широкой проблемы — безопасности компьютерных систем, или еще более общей проблемы — информационной безопасности. Информация, как продукт, удовлетворяющий определенным потребностям субъектов, который они получают посредством информационных систем, должна обладать следующими свойствами.

Доступность — возможность за приемлемое время выполнить ту или иную операцию над данными или получить нужную информацию.

Целостность — это актуальность и непротиворечивость хранимой информации.

Непротиворечивость информации — это соответствие содержимого информационном базы логике предметной области.

Конфиденциальность — защищенность информации от несанкционированного доступа.

Проблема обеспечения защиты информации является одной из важнейших при построении надежной информационной структуры учреждения на базе ЭВМ. Эта проблема охватывает как физическую защиту данных и системных программ, так и защиту от несанкционированного доступа к данным, передаваемым по линиям связи и находящимся на накопителях, являющегося результатом деятельности, как посторонних лиц, так и специальных программ-вирусов.

В настоящее время в современном мире электронных технологий практически невозможно представить компанию, в которой не требуется обработка некоторого объёма информации. Информацию требуется, где-то хранить. Информация может динамически изменяться. Регулярно требуется выборка данных по определённым критериям. Базы данных – это часть информационных систем, программно-аппаратных комплексов, осуществляющих хранение и обработку огромных информационных массивов.

## ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

### Связь работы с приоритетными направлениями научных исследований

Тема диссертационной работы соответствует подразделу 13 «Безопасность человека, общества, государства» приоритетных направлений научных исследований Республики Беларусь на 2016-2020 гг., утвержденных Постановлением Совета Министров Республики Беларусь 12 марта 2015 г, №190. Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

### Цель и задачи исследования

На основе известных методов обеспечения безопасности систем управления реляционными базами данных разработать обобщённую методику защиты информации в реляционных СУБД.

Для достижения поставленной цели необходимо было выполнить следующие задачи:

1. Выявить наиболее существенные уязвимости в реляционных СУБД.
2. С учётом этого сформулировать политику информационной безопасности в реляционных СУБД.
3. Разработать обобщённую методику информационного аудита реляционных СУБД.

### Апробация результатов диссертации

Основные положения и результаты диссертации обсуждались на 53-ей научной конференции аспирантов, магистрантов и студентов (Минск,2017).

### Опубликованность результатов диссертации

По результатам исследований, представленных в диссертации, опубликована 1 работа, в том числе 1 статья в сборниках материалов конференции.

### Личный вклад

Личное участие автора диссертации охватывает исследования по построению и обеспечению безопасности систем управления реляционными базами данных. Автором проведен анализ существующих методик по описанным направлениям, разработка обобщённой методики по обеспечению безопасности на основе существующих методик, сформулированы общие положения диссертации, составляющие практическую значимость.

# КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

## Сущность понятия безопасности баз данных

Достаточно четко сформулировать понятие безопасности некоторой системы не просто. Ставить же задачу обеспечения безопасности функционирования какой-либо системы, не определив само понятие безопасности, неправильно, так как отсутствие ясного понимания цели проекта обычно ведёт к нерациональному использованию ресурсов и, возможно, к срыву всего проекта. Поэтому на государственном уровне сформулированы и законодательно оформлены документы, определяющие концепцию безопасности и концепцию экономической безопасности.

В этих документах, а также во многих научных работах понятие безопасности связывается с защитой некоторых активов от угроз. Угрозы классифицируются в зависимости от возможности нанесении ущерба защищаемым активом. В качестве основных обычно рассматриваются угрозы, которые связаны с умышленными действиями или непреднамеренными действиями людей. Помимо угроз, связанных с деятельностью человека, существуют и рассматриваются угрозы, связанные с объективными процессами, происходящими в природе, такими, как стихийные бедствия, физически процессы, влияющие на распространение радиоволн, и т.п.

Безопасность ИТКС можно определить как состояние защищённости ИТКС от угроз её нормальному функционированию. Под защищённостью понимается наличие средств ИТКС и методов их применения, обеспечивающих снижение или ликвидацию негативных последствий, связанных с реализацией угроз. Изложенный подход к определению понятия безопасности ИТКС предполагает, что перечень и содержание угроз достаточно хорошо определены и достаточно стабильны во времени.

Безопасность ИТКС можно определить, как свойство системы адаптироваться к агрессивным проявлениям среды, в которой функционирует система, обеспечивающее поддержку на экономически оправданном уровне характеристики качества системы. В сформулированном определении основной акцент делается не на перечне и содержании угроз, нейтрализация которых обеспечивается, а на особую характеристику качества системы. При этом основной критерий качества ИТКС 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.

Уверенность в безопасности ИТКС может быть достигнута в результате согласованных действий, предпринимаемых в процессе разработки, оценки и эксплуатации объекта оценки. Функциональное назначение оценки безопасности ИТКС – получение определенной степени уверенности в том, насколько система удовлетворяет предъявляемым к ним требованиям. Результаты оценки должны помочь потребителю установить, достаточен ли уровень безопасности системы для предполагаемых применений этой системы и являются ли приемлемыми остаточные риски.

Уязвимость ИТКС - это некая ее характеристика, которая делает возможным существование угрозы. Другими словами, именно из-за наличия уязвимостей в системе могут происходить нежелательные события.

Атака на ИТКС - это действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости для реализации некоторой угрозы ИБ ИТКС. Таким образом, под атакой будем понимать процесс реализации угрозы. Заметим, что такое толкование атаки (с участием человека, имеющего злой умысел), исключает присутствующий в определении угрозы элемент случайности, но, как показывает опыт, часто бывает невозможно различить преднамеренные и случайные действия, и система защиты должна адекватно реагировать на любое из них.

Угрозы, связанные с несанкционированным доступом, выделяются из всего комплекса угроз по способу реализации. При этом под несанкционированным доступом понимается доступ к информации заинтересованным субъектом с нарушением установленных прав или правил доступа к информации. Сам несанкционированный доступ угрозой как таковой не является. Угрозы могут появиться в связи с НСД. При этом может быть несанкционированное ознакомление с информацией, несанкционированное копирование (хищение) информации и/или несанкционированное воздействие на информацию (уничтожение, блокирование и т.д.).

**Методы и средства обеспечения безопасности**

Задача обеспечения информационной безопасности должна решаться системно. Это означает, что различные средства защиты (аппаратные, программные, физические, организационные и т. д.) должны применяться одновременно и под централизованным управлением.

На сегодняшний день существует большой арсенал методов обеспечения информационной безопасности:

– средства идентификации и аутентификации пользователей;

– средства шифрования информации, хранящейся на компьютерах и передаваемой по сетям;

– межсетевые экраны;

– виртуальные частные сети;

– средства контентной фильтрации;

– инструменты проверки целостности содержимого дисков;

– средства антивирусной защиты;

– системы обнаружения уязвимостей сетей и анализаторы сетевых атак.

Каждое из перечисленных средств может быть использовано как самостоятельно, так и в интеграции с другими. Это делает возможным создание систем информационной защиты для сетей любой сложности и конфигурации, не зависящих от используемых платформ.

Таким образом, существует большое количество различных методов обеспечения информационной безопасности. Наиболее эффективным является применение всех данных методов в едином комплексе.

Необходимо регулярно проводить оценку защищённости ИТКС, для того чтобы быстро реагировать на угрозы направленные на информационные системы.

В общем случае оценка уровня защищённости состоит из ряда последовательных этапов рисунок 1, каждый из которых предусматривает выполнение определённого круга задач.

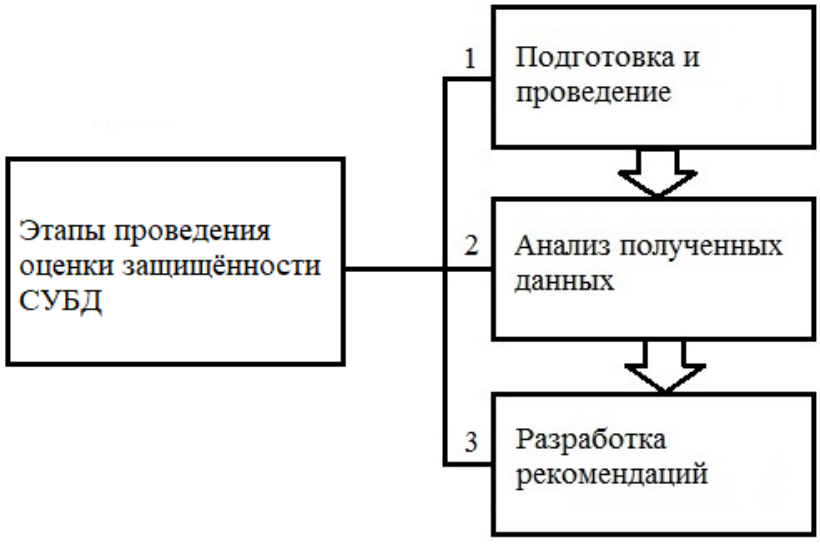


**Рисунок 1 - Этапы проведения оценки защищённости СУБД**

На первом этапе осуществляется подготовка к оценке защищённости, которая включает в себя сбор исходной информации. Качество проводимого оценки безопасности во многом зависит от полноты и точности информации, которая была получена в процессе сбора исходных данных. Поэтому информация должна включать в себя: существующую организационно-распорядительную документацию, касающуюся вопросов информационной безопасности, сведения о программно-аппаратном обеспечении ИТКС, информацию о средствах защиты, установленных в ИТКС и т.д.

На втором этапе, после сбора необходимой информации, проводится её анализ с целью оценки текущего уровня защищённости системы. В процессе проведения оценки защищённости безопасности могут использоваться специализированные программные комплексы, позволяющие автоматизировать процесс анализа исходных данных и расчёта значений рисков.

На третьем этапе проведения аудита разрабатываются рекомендации по совершенствованию безопасности. Как правило, разработанные рекомендации направлены не на полное устранение всех выявленных рисков, а лишь на их уменьшение до приемлемого остаточного уровня. При выборе мер по повышению уровня защиты ИТКС учитывается одно принципиальное ограничение – стоимость их реализации не должна превышать стоимость защищаемых информационных ресурсов.

# ЗАКЛЮЧЕНИЕ

Информационная безопасность относится к числу дисциплин, развивающихся чрезвычайно быстрыми темпами. Этому способствуют как общий прогресс информационных технологий, так и постоянное противоборство нападающих и защищающихся.

К сожалению, подобная динамичность объективно затрудняет обеспечение надежной защиты.

Обеспечение информационной безопасности современных информационных систем требует комплексного подхода. Оно невозможно без применения широкого спектра защитных средств, объединенных в продуманную архитектуру. Далеко не все эти средства получили распространение в РБ, некоторые из них даже в мировом масштабе находятся в стадии становления.

## СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1-А. Конопелько И.А. Защита в СУБД информации // Доклад к 53-ой научной конференции аспирантов, магистрантов и студентов – БГУИР – Минск, 2017.