

МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учебно-методическое объединение по образованию
в области информатики и радиоэлектроники

УТВЕРЖДАЮ

Первый заместитель Министра образования
Республики Беларусь

_____ А.Г. Баханович

Регистрационный № _____

БЕЗОПАСНОСТЬ БАЗ ДАННЫХ

**Примерная учебная программа по учебной дисциплине
для специальности**

7-06-0611-02 Информационная безопасность

СОГЛАСОВАНО

Председатель Учебно-
методического объединения по
образованию в области
информатики и радиоэлектроники

_____ В.А. Богуш

СОГЛАСОВАНО

Начальник Главного управления
профессионального образования
Министерства образования
Республики Беларусь

_____ С.Н. Пищов

СОГЛАСОВАНО

Проректор по научно-методической
работе Государственного учреждения
образования «Республиканский
институт высшей школы»

_____ И.В. Титович

Эксперт-нормоконтролер

СОСТАВИТЕЛИ:

А.А.Бутов, доцент кафедры экономической информатики учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», кандидат технических наук, доцент;

В.Н.Комличенко, доцент кафедры экономической информатики учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», кандидат технических наук, доцент

РЕЦЕНЗЕНТЫ:

Кафедра автоматизированных систем управления производством учреждения образования «Белорусский государственный аграрный технический университет» (протокол № 12 от 27.05.2025);

В.А.Грушев, заместитель директора по производству иностранного унитарного предприятия «САМСОЛЮШНС», кандидат технических наук

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ В КАЧЕСТВЕ ПРИМЕРНОЙ:

Кафедрой экономической информатики учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» (протокол № 15 от 02.05.2025);

Научно-методическим советом учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» (протокол № ____ от _____);

Научно-методическим советом по информационной безопасности Учебно-методического объединения по образованию в области информатики и радиоэлектроники (протокол № 12 от 02.06.2025)

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

ХАРАКТЕРИСТИКА УЧЕБНОЙ ДИСЦИПЛИНЫ

Примерная учебная программа по учебной дисциплине «Безопасность баз данных» разработана для магистрантов учреждений высшего образования, обучающихся по специальности 7-06-0611-02 «Информационная безопасность» в соответствии с требованиями образовательного стандарта углубленного высшего образования и примерного учебного плана вышеуказанной специальности.

Системы управления базами данных (СУБД) стали важнейшим инструментом в области хранения, обработки и представления данных. Любой сбой в работе СУБД, сопровождающийся потерей, хоть и временной, доступа к данным, немедленно отражается на конкурентной способности предприятия. Поэтому защита данных от несанкционированного доступа, несанкционированной модификации или от разрушения является одной из приоритетных задач при проектировании любой информационной системы.

Изучение настоящей учебной дисциплины обеспечивает подготовку специалиста, владеющего фундаментальными знаниями и практическими навыками в области проектирования баз данных, обеспеченных современными средствами защиты хранимых данных от хищения, искажения или потери, а также умеющего работать с данными с помощью языка структурированных запросов SQL.

Воспитательное значение учебной дисциплины «Безопасность баз данных» заключается в формировании у обучающихся математической культуры и научного мировоззрения; развитии исследовательских умений, аналитических способностей, креативности, необходимых для решения научных и практических задач; развитии познавательных способностей и активности: творческой инициативы, самостоятельности, ответственности и организованности; формировании способностей к саморазвитию, самосовершенствованию и самореализации.

Изучение данной учебной дисциплины способствует созданию условий для формирования интеллектуально развитой личности обучающегося, которой присущи стремление к профессиональному совершенствованию, активному участию в экономической и социально-культурной жизни страны, гражданская ответственность и патриотизм.

ЦЕЛЬ, ЗАДАЧИ УЧЕБНОЙ ДИСЦИПЛИНЫ

Цель учебной дисциплины: освоение знаний по вопросам, связанным с теорией и проектирования современных баз данных с ориентацией на обеспечение информационной безопасности, целостности и доступности хранимых данных, защиты их от искажения или разрушения.

Задачи учебной дисциплины:

приобретение знаний об основных принципах проектирования баз данных, причинах их уязвимостей и источниках угроз информационной безопасности, о последовательности действий по обеспечению безопасности баз данных;

изучение принципов логического и физического проектирования баз данных, создания защищенных баз данных, поддержания целостности данных, восстановления поврежденных данных;

приобретение навыков разработки баз данных, снабженных средствами защиты данных, для решения прикладных задач обработки данных;

овладение методами управления доступом к данным, способами защиты данных с помощью представлений, хранимых процедур и функций, принципами проектирования программных средств, защищенных от SQL-инъекций, приемами достижения оптимальной производительности при работе с базами данных.

Базовыми учебными дисциплинами для учебной дисциплины «Безопасность баз данных» являются «Менеджмент информационной безопасности», «Организация данных в сетевых приложениях». В свою очередь учебная дисциплина «Безопасность баз данных» является базой для таких учебных дисциплин компонента учреждения образования, как «Защита веб-ресурсов от несанкционированного доступа», «Проектирование систем защиты объектов информатизации», «Технологии распределенной обработки и хранения данных».

ТРЕБОВАНИЯ К УРОВНЮ ОСВОЕНИЯ СОДЕРЖАНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

В результате изучения учебной дисциплины «Безопасность баз данных» формируется следующая углубленная профессиональная компетенция: разрабатывать базы данных для решения прикладных задач в сфере защиты информации.

В результате изучения учебной дисциплины обучающийся должен:

знать:

основные принципы проектирования современных баз данных;

причины уязвимостей баз данных и источники угроз информационной безопасности;

последовательность действий по обеспечению безопасности баз данных;

уметь:

создавать логические и физические модели данных;

использовать команды языка структурированных запросов SQL для создания объектов базы данных и манипулирования информацией, содержащейся в ней;

оценивать угрозы информационной безопасности и их причины;

применять методы и средства обеспечения безопасности баз данных;

иметь навык:

управления доступом к данным;
поддержания целостности данных;
восстановления поврежденных данных;
защиты данных с помощью представлений, хранимых процедур и функций;
проектирования и настройки программных средств для обеспечения защиты данных от несанкционированного доступа.

Примерная учебная программа рассчитана на 120 учебных часов, из них – 58 аудиторных. Примерное распределение аудиторных часов по видам занятий: лекции – 34 часа, лабораторные занятия – 24 часа.

ПРИМЕРНЫЙ ТЕМАТИЧЕСКИЙ ПЛАН

Наименование раздела, темы	Всего аудиторных часов	Лекции	Лабораторные занятия
Раздел 1. Основы теории проектирования баз данных	12	8	4
Тема 1. Логическое проектирование баз данных	4	2	2
Тема 2. Физическое проектирование баз данных	8	6	2
Раздел 2. Обеспечение безопасности баз данных	38	22	16
Тема 3. Основы информационной безопасности и анализ уязвимостей баз данных	6	2	4
Тема 4. Специфика получения несанкционированного доступа к данным	4	4	-
Тема 5. Управление доступом к данным	8	4	4
Тема 6. Обеспечение целостности данных	2	2	-
Тема 7. Восстановление поврежденных данных	4	2	2
Тема 8. Защита данных с помощью представлений, хранимых процедур и функций, триггеров	8	4	4
Тема 9. Обеспечение конфиденциальности информации, хранимой в базе данных	6	4	2
Раздел 3. Практические способы обеспечения безопасности	8	4	4
Тема 10. Реализация системы защиты в СУБД Access	4	2	2
Тема 11. Архитектура системы безопасности СУБД SQL Server	4	2	2
Итого:	58	34	24

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Раздел 1. ОСНОВЫ ТЕОРИИ ПРОЕКТИРОВАНИЯ БАЗ ДАННЫХ

Тема 1. ЛОГИЧЕСКОЕ ПРОЕКТИРОВАНИЕ БАЗ ДАННЫХ

Основные понятия, лежащие в основе концепции баз данных. Жизненный цикл базы данных. Модель данных и ее реализация. Логические модели данных. Определение и свойства сущности. Определение возможного ключа. Первичный и альтернативный ключи. Типы связей между сущностями. Нормализация данных. CASE-средства для моделирования структур данных. Диаграммы «сущность-связь».

Тема 2. ФИЗИЧЕСКОЕ ПРОЕКТИРОВАНИЕ БАЗ ДАННЫХ

Физическая организация баз данных. Системы управления базами данных. Назначение и функции СУБД. Язык структурированных запросов SQL. Распределенные базы данных. Системы поддержки принятия решений. Хранилища данных.

Раздел 2. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ БАЗ ДАННЫХ

Тема 3. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И АНАЛИЗ УЯЗВИМОСТЕЙ БАЗ ДАННЫХ

Классификация угроз информационной безопасности и их причины. Источники угроз информационной безопасности. Основные принципы обеспечения информационной безопасности баз данных.

Тема 4. СПЕЦИФИКА ПОЛУЧЕНИЯ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ДАННЫМ

Инференция и агрегирование. Использование разрешенных запросов для получения закрытых данных. Скрытые каналы передачи информации. SQL-инъекции. Программные закладки, отладочный код. Троянские кони.

Тема 5. УПРАВЛЕНИЕ ДОСТУПОМ К ДАННЫМ

Организационные меры обеспечения безопасности информации. Идентификация, аутентификация и авторизация пользователей. Дискреционное, мандатное и ролевое управление доступом к данным.

Тема 6. ОБЕСПЕЧЕНИЕ ЦЕЛОСТНОСТИ ДАННЫХ

Принципы обеспечения целостности данных. Модель целостности Кларка-Вильсона. Модель Биба. Совместное использование моделей безопасности. Задание ограничений целостности с помощью операторов языка SQL.

Тема 7. ВОССТАНОВЛЕНИЕ ПОВРЕЖДЕННЫХ ДАННЫХ

Понятие транзакции и журнала транзакций. Принципы и методы восстановления данных. Создание отказоустойчивых систем.

Теми 8. ЗАЩИТА ДАННЫХ С ПОМОЩЬЮ ПРЕДСТАВЛЕНИЙ, ХРАНИМЫХ ПРОЦЕДУР И ФУНКЦИЙ, ТРИГГЕРОВ

Определение представления, его свойства, специфика использования. Понятие хранимой процедуры, параметры процедуры, выполнение. Хранимая функция, ее виды, выполнение. Определение триггера, принцип работы.

Тема 9. ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ, ХРАНИМОЙ В БАЗЕ ДАННЫХ

Шифрование данных. Регистрация обращений к защищаемым ресурсам (протоколирование). Организация аудита базы данных. Обработка данных аудита.

Раздел 3. ПРАКТИЧЕСКИЕ СПОСОБЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Тема 10. РЕАЛИЗАЦИЯ СИСТЕМЫ ЗАЩИТЫ В СУБД ACCESS

Обеспечение защиты на уровне пользователя. Методы противодействия взлому защиты в СУБД Access.

Тема 11. АРХИТЕКТУРА СИСТЕМЫ БЕЗОПАСНОСТИ СУБД SQL SERVER

Реализация системы безопасности на уровне сервера. Аутентификация Windows. Аутентификация SQL Server. Реализация системы безопасности на уровне базы данных.

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ**ЛИТЕРАТУРА****ОСНОВНАЯ**

1. Дейт, К. Д. Введение в системы баз данных / К. Д. Дейт ; пер. с англ. – 8-е изд. – Москва : Вильямс, 2006. – 1328 с.
2. Дейт, К. Д. SQL и реляционная теория : как грамотно писать код на SQL / К. Д. Дейт ; пер. А. Слинкина. – Санкт-Петербург ; Москва : Символ, 2014. – 480 с.
3. Садаладж, П. Д. NoSQL : новая методология разработки нереляционных баз данных / П. Д. Садаладж, М. Фаулер. – Москва : Вильямс, 2017. – 192 с.
4. Маклаков, С. В. Создание информационных систем с AllFusion Modeling Suite / С. В. Маклаков. – Москва : Диалог-Мифи, 2005. – 432 с.
5. Бондарь, А. Г. Microsoft SQL Server 2012 / А. Г. Бондарь. – Санкт-Петербург : БХВ-Петербург, 2013. – 608 с.
6. Сеннов, А. С. Access 2010 : учебный курс / А. С. Сеннов. – Санкт-Петербург : Питер, 2010. – 288 с.
7. Информационная безопасность открытых систем : учебник : в 2 т. Т. 1 : Угрозы, уязвимости, атаки и подходы к защите / С. В. Запечников [и др.]. – Москва : Горячая линия-Телеком, 2006. – 536 с.
8. Информационная безопасность открытых систем : учебник : в 2 т. Т. 2 : Средства защиты в сетях / С. В. Запечников [и др.]. – Москва : Горячая линия-Телеком, 2008. – 558 с.
9. Основы информационной безопасности : учебное пособие / Е. Б. Белов [и др.]. – Москва : Горячая линия-Телеком, 2006. – 544 с.
10. Галатенко, В. А. Основы информационной безопасности : курс лекций / В. А. Галатенко ; под ред. В. Б. Бетелина. – Москва : Интернет-Университет Информационных Технологий, 2003. – 280 с.
11. Цирлов, В. Л. Основы информационной безопасности автоматизированных систем. – Ростов на Дону : Феникс, 2008. – 173 с.

ДОПОЛНИТЕЛЬНАЯ

12. Голицына, О. Л. Базы данных : учебное пособие / О. Л. Голицына, Н. В. Максимов, И. И. Попов. – 4-е изд., перераб. и доп. – Москва : ФОРУМ : ИНФРА-М, 2016. – 400 с.
13. Кузнецов, С. Д. Базы данных. Модели и языки : учебник / С. Д. Кузнецов. – Москва : Бином, 2008. – 720 с.
14. Советов, Б. Я. Базы данных : теория и практика : учебник / Б. Я. Советов, В. В. Цехановский, В. Д. Чертовской. – Москва : Высшая школа, 2007. – 463 с.
15. Фрост, Р. Проектирование и разработка баз данных : визуальный подход / Р. Фрост, Д. Дей, К. Ван Слайк. – Москва : НТ Пресс, 2007. – 592 с.
16. Марков, А. С. Базы данных : введение в теорию и методологию : учебник / А. С. Марков, К. Ю. Лисовский. – Москва : Финансы и статистика, 2006. – 512 с.

17. Малыхина, М. П. Базы данных : основы, проектирование, использование : учебное пособие / М. П. Малыхина. – 2-е изд. – Санкт-Петербург : БХВ-Петербург, 2006. – 528 с.

18. Кляйн, К. SQL : справочник / К. Кляйн, Д. Кляйн, Б. Хант ; пер. с англ. – 3-е изд. – Санкт-Петербург : Символ-Плюс, 2010. – 656 с.

19. Андон, Ф. Язык запросов SQL : учебный курс / Ф. Андон, В. Резниченко. – Санкт-Петербург : Питер, 2006. – 416 с.

20. Маклаков, С. В. ВРwin и ERwin. CASE-средства разработки информационных систем / С. В. Маклаков. – Москва : Диалог-Мифи, 2000. – 256 с.

21. Хотек, М. Microsoft SQL Server 2008. Реализация и обслуживание : учебный курс / М. Хотек ; пер. с англ. – Москва : Русская редакция, 2011. – 576 с.

22. Хомоненко, А. Д. Access : экспресс-курс / А. Д. Хомоненко, В. Гридин. – Санкт-Петербург : БХВ-Петербург, 2005. – 304 с.

23. Шкарина, Л. Н. Язык SQL : учебный курс / Л. Н. Шкарина. – Санкт-Петербург : Питер, 2003. – 592 с.

24. Смирнов, С. Н. Безопасность систем баз данных / С. Н. Смирнов. – Москва : Гелиос АРВ, 2007. – 352 с.

25. Марков, А. С. Методы оценки несоответствия средств защиты информации / А. С. Марков, В. Л. Цирлов, А. В. Барабанов; под ред. А. С. Маркова. – Москва : Радио и связь, 2012. – 192 с.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ И ВЫПОЛНЕНИЮ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЩАЮЩИХСЯ

При изучении учебной дисциплины рекомендуется использовать следующие формы самостоятельной работы:

работа с технической литературой;

составление конспектов;

подготовка к выполнению лабораторных работ;

составление отчетов по лабораторным работам;

участие в научно-исследовательской и методической работе, проводимой на кафедре;

участие в конкурсах научных работ и научных конференциях;

работа с методическим материалом.

ПЕРЕЧЕНЬ РЕКОМЕНДУЕМЫХ СРЕДСТВ ДИАГНОСТИКИ КОМПЕТЕНЦИЙ ОБУЩАЮЩИХСЯ

Примерным учебным планом по специальности 7-06-0611-02 «Информационная безопасность» в качестве формы промежуточной аттестации по учебной дисциплине «Безопасность баз данных» рекомендуется экзамен. Оценка учебных достижений обучающихся производится по десятибалльной шкале.

Для текущего контроля по учебной дисциплине и диагностики компетенций могут использоваться следующие формы:

устный и письменный опрос;

письменная самостоятельная работа;
составление тестов и эталонов ответов к ним;
собеседование при проведении индивидуальных и групповых консультаций;
защита лабораторных работ.

РЕКОМЕНДУЕМЫЕ МЕТОДЫ (ТЕХНОЛОГИИ) ОБУЧЕНИЯ

Основные рекомендуемые методы (технологии) обучения, отвечающие целям и задачам учебной дисциплины:

компьютерное обучение;
элементы проблемного обучения (проблемное изложение, вариативное изложение, частично-поисковый метод), реализуемые на лекционных занятиях;
элементы учебно-исследовательской деятельности, реализуемые на лабораторных занятиях.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ТЕМ ЛАБОРАТОРНЫХ ЗАНЯТИЙ

1. Разработка логической и физической моделей данных с помощью программы ERwin (или аналогичной). Выполнение операций прямого и обратного проектирования.
2. Создание средствами языка SQL сценария для генерации базы данных и ее объектов с наполнением ее таблиц конкретными данными.
3. Управление доступом к данным путем использования механизмов аутентификации, регистрации пользователей, назначения ролей, привилегий и запретов.
4. Резервное копирование и восстановление данных. Порядок выполнения действий по восстановлению поврежденных данных средствами СУБД.
5. Защита данных средствами языка SQL. Создание и использование для усиления защиты данных хранимых на сервере процедур, пользовательских функций и триггеров.
6. Обеспечение конфиденциальности данных. Изучение функций шифрования данных. Использование программы ScanOVAL для поиска и анализа уязвимостей базы данных.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ КОМПЬЮТЕРНЫХ ПРОГРАММ

(необходимого оборудования, наглядных пособий и др.)

1. Операционная система Microsoft Windows 10 или выше.
2. CASE-средство разработки информационных систем Erwin (или аналогичное).
3. Реляционная система управления базами данных.
4. Система управления не реляционными базами данных.