

Белорусский государственный университет

УТВЕРЖДАЮ

Проректор по учебной работе

А.Л. Толстик

16 декабря 2016

Регистрационный № УД- 3538 / уч.



Защита информации в базах данных и экспертных системах

Учебная программа учреждения высшего образования
по учебной дисциплине для специальности:

1-98 01 01 Компьютерная безопасность (по направлениям)
Направление специальности: 1-98 01 01-02 Компьютерная безопасность
(радиофизические методы и программно-технические средства);

2016 г.

Учебная программа составлена на основе *образовательного стандарта высшего образования по специальности 1-98 01 01 Компьютерная безопасность ОСВО 1-98 01 01-2013 и учебных планов УВО № Р98-139/уч. 2013 г., № Р98и-140/уч. 2013 г.*

СОСТАВИТЕЛИ:

Виктор Васильевич Скакун, заведующий кафедрой системного анализа и компьютерного моделирования, кандидат физико-математических наук, доцент.

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой системного анализа и компьютерного моделирования Белорусского государственного университета
(протокол № 12 от 14 июня 2016 г.);

Учебно-методической комиссией факультета радиофизики и компьютерных технологий Белорусского государственного университета
(протокол № 4 от 20 декабря 2016 г).

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Учебная программа дисциплины специализации «Защита информации в базах данных и экспертных системах» разработана для студентов специальности 1-98 01 01-02 Компьютерная безопасность (радиофизические методы и программно-технические средства) в соответствии с требованиями Образовательного стандарта ОСВО 1-31 04 03-2013 и учебных планов УВО № Р98-139/уч. 2013 г., № Р98и-140/уч. 2013 г.

Дисциплина «Защита информации в базах данных (БД) и экспертных системах (ЭС)» имеет целью раскрыть содержание основных понятий, методов и механизмов обеспечения информационной безопасности БД и ЭС. Содержание дисциплины определяется апробированными в практической реализации методами и механизмами обеспечения конфиденциальности, целостности и доступности информации в БД и ЭС. Задачи дисциплины – дать основы системного и комплексного подхода к анализу и обеспечению информационной безопасности БД и ЭС в процессах их создания и эксплуатации (администрирования), а также представления, анализа и обоснования моделей, методов и механизмов обеспечения информационной безопасности БД и ЭС.

Практическая часть заключается в овладении навыками разработки защищенной БД в СУБД MS Access и MS SQL Server и навыками их администрирования. Дисциплина «Защита информации в базах данных и экспертных системах» опирается на материал дисциплин «Программирование» и «Модели данных и СУБД», изучаемых на факультете и составлена с учетом межпредметных связей с данными дисциплинами.

В результате усвоения дисциплины студент должен:

знать:

- основные понятия и составляющие информационной безопасности БД и ЭС;
- систематику методов и механизмов обеспечения информационной безопасности БД и ЭС;
- обязательные, избирательные и ролевые модели разграничения доступа к информации в БД;
- технологии индивидуально-группового доступа к разделяемым информационным ресурсам: методы и технологии обеспечения сохранности и правомерной доступности информации в БД и ЭС.

уметь:

- анализировать функциональную и системную архитектуру БД и ЭС в контексте обеспечения информационной безопасности;
- применять системные процедуры и инструкции языка SQL для реализации установок избирательного и ролевого доступа, обеспечения целостности данных; программировать представления, триггеры, функции и сохраненные процедуры;
- вырабатывать перечень процедур и работ по администрированию защищенных БД и ЭС;
- творчески и эффективно использовать полученные знания в своей профессиональной деятельности.

владеть:

- навыками программирования на языке SQL установок избирательного и ролевого доступа, обеспечения целостности и доступности данных;
- навыками программирования представлений, триггеров, функций и сохраненных процедур на языке Transact SQL;
- навыками разработки и программной реализации защищенных клиент-серверных баз данных с использованием СУБД MS Access и MS SQL Server.

Изучение учебной дисциплины «Защита информации в базах данных и экспертных системах» должно обеспечить формирование у студента следующих компетенций:

- АК-1. Уметь применять базовые научно-теоретические знания для решения теоретических и практических задач,
- АК-2. Владеть системным и сравнительным анализом,
- АК-4. Уметь работать самостоятельно,
- АК-6. Владеть междисциплинарным подходом при решении проблем,
- АК-7. Иметь навыки, связанные с использованием технических устройств, управлением информацией и работой с компьютером,
- ПК-3. Разрабатывать модели явлений, процессов или систем при организации защиты информации,
- ПК-8. Разрабатывать и совершенствовать методы исследований в области информационных и телекоммуникационных систем,
- ПК-9. Анализировать и оценивать собранные данные,
- ПК-12. Пользоваться глобальными информационными ресурсами,
- ПК-13. Владеть современными средствами телекоммуникаций,
- ПК-27. Разрабатывать новые информационные технологии на основе математического моделирования и оптимизации.

В соответствии с учебным планом объем дисциплины составляет 116 учебных часов (3.5 зачетных единиц), в том числе 62 аудиторных часа, из них лекции – 34, лабораторные работы – 28.

Дисциплина «Защита информации в базах данных и экспертных системах» изучается студентами дневной формы получения высшего образования на 4-ом курсе в 8 семестре.

Форма текущей аттестации по учебной дисциплине – зачет.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

1. **ВВЕДЕНИЕ И ОСНОВНЫЕ ПОНЯТИЯ**
Введение. Основные понятия. Субъекты и объекты безопасности. Общая характеристика составляющих информационной безопасности. Угрозы и нарушители безопасности. Классификация угроз информационной безопасности. Характеристика основных уязвимостей. Основные принципы обеспечения информационной безопасности. Специфика защиты в базах данных. SQL инъекции: примеры реализации и способы противодействия.
2. **ЭКСПЕРТНЫЕ СИСТЕМЫ**
Базовая структура экспертной системы. Отличие ЭС от БД. Представление знаний в экспертной системе. Модели представления. Организация и вывод знаний.
3. **УПРАВЛЕНИЕ ДОСТУПОМ К ДАННЫМ**
Идентификация, аутентификация и авторизация пользователей. Избирательный подход к разграничению доступа. Матрица доступа. Модель Харрисона-Руззо-Ульмана. Элементы языка SQL управления доступом. Обязательный (мандатный) подход к разграничению доступа к данным. Уровни безопасности. Модель Белла-ЛаПадуллы и ее расширения. Ролевая модель разграничения доступа. Модель «китайской стены».
4. **МОДЕЛИ И МЕТОДЫ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ, СОХРАННОСТИ И ПРАВОМЕРНОЙ ДОСТУПНОСТИ ДАННЫХ**
Принципы обеспечения целостности данных. Модели обеспечения целостности данных. Модель Кларка-Вильсона. Модель Биба. Совместное использование моделей безопасности и целостности. Методы управления транзакциями. Уровни изоляции транзакций. Операторы языка SQL контроля целостности и управления транзакциями. Журнал транзакций. Виды сбоев. Методы восстановления информации после локального, мягкого и жесткого сбоев. Организация восстановления данных в СУБД MS SQL Server. Создание отказоустойчивых систем. RAID массивы.
5. **ЗАЩИТА ДАННЫХ С ПОМОЩЬЮ ПРЕДСТАВЛЕНИЙ, СОХРАНЕННЫХ ПРОЦЕДУР, ФУНКЦИЙ И ТРИГГЕРОВ**
Обеспечение безопасности и секретности данных с помощью представлений, хранимых процедур, функций и триггеров. Доступ к данным через представления. Свойства представлений. Основы языка Transact SQL. Программирование хранимых процедур, функций и триггеров в Transact SQL.
6. **ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ И СЕКРЕТНОСТИ ДАННЫХ В СУБД MS ACCESS И MS SQL SERVER**
Система безопасности MS Access. Методы противодействия взлому защиты Access. Архитектура безопасности MS SQL Server. Система безопасности уровня сервера. Аутентификация и SQL Server. Фиксированные роли сервера. Система безопасности уровня БД. Фиксированные и пользовательские роли БД. Администрирование БД в MS SQL Server.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов					Количество часов УСР	Форма контроля знаний
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное		
1	2	3	4	5	6	7	8	9
1.	ВВЕДЕНИЕ И ОСНОВНЫЕ ПОНЯТИЯ	6						
1.1	<i>Введение.</i> Основные понятия и определения. Субъекты и объекты безопасности. Общая характеристика составляющих информационной безопасности.	2						Устный опрос
1.2	Угрозы безопасности. Нарушители безопасности. Классификация угроз информационной безопасности. Понятие уязвимости систем защиты. Характеристика основных уязвимостей. Основные принципы обеспечения информационной безопасности.	2						Устный опрос
1.3	Специфика защиты в базах данных. Инференция и агрегирование, скрытые каналы передачи данных. SQL инъекции: примеры реализации и способы противодействия.	2			4			Отчет по лабораторной работе
2	ЭКСПЕРТНЫЕ СИСТЕМЫ	2						
2.1	Базовая структура экспертной системы. Отличие ЭС от БД. Представление знаний в экспертной системе. Модели представления знаний на основе семантических сетей, фреймов и логических выражений. Организация и вывод знаний.	2						Устный опрос
3	УПРАВЛЕНИЕ ДОСТУПОМ К ДАННЫМ	6						
3.1	Идентификация, аутентификация и авторизация пользователей. Избирательный (дискреционный) подход к разграничению доступа. Матрица доступа. Принудительное и добровольное управление доступом.	2						Устный опрос
3.2	Модель Харрисона-Руззо-Ульмана. Элементы языка SQL управления доступом.	2						Устный опрос
3.3	Обязательный (мандатный) подход к разграничению доступа к данным. Уровни (решетка) безопасности. Модель Белла-ЛаПадуллы и ее расширения. Ролевая модель разграничения доступа. Модель «китайской стены».	2						Устный опрос

4	МОДЕЛИ И МЕТОДЫ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ, СОХРАННОСТИ И ПРАВОМЕРНОЙ ДОСТУПНОСТИ ДАННЫХ	8						
4.1	Принципы обеспечения целостности данных. Модели обеспечения целостности данных. Модель Кларка-Вильсона. Модель Биба. Совместное использование моделей безопасности и целостности.	2						Устный опрос
4.2	Изменение данных как событие. Контроль целостности данных на основе триггеров и хранимых процедур. Методы управления транзакциями. Уровни изоляции транзакций. Операторы языка SQL контроля целостности и управления транзакциями.	2			4			Отчет по лабораторной работе.
4.3	Журнал транзакций. Виды сбоев. Методы восстановления информации после локального, мягкого и жесткого сбоев. Резервирование БД.	2						Устный опрос
4.4	Организация восстановления данных в СУБД MS SQL Server. Создание отказоустойчивых систем. RAID массивы.	2			2			Отчет по лабораторной работе
5	ЗАЩИТА ДАННЫХ С ПОМОЩЬЮ ПРЕДСТАВЛЕНИЙ, СОХРАНЕННЫХ ПРОЦЕДУР, ФУНКЦИЙ И ТРИГГЕРОВ	6						
5.1	Обеспечение безопасности и секретности данных с помощью представлений, хранимых процедур, функций и триггеров. Доступ к данным через представления. Свойства представлений. Обновление данных в представлениях.	2						Устный опрос
5.2	Основы языка Transact SQL. Элементы Transact SQL для программирования хранимых процедур, функций и триггеров.	2						Устный опрос
5.3	Программирование процедур, функций и триггеров.	2			4			Отчет по лабораторной работе
6	ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ И СЕКРЕТНОСТИ ДАННЫХ В СУБД MS ACCESS И MS SQL SERVER	6						
6.1	Система безопасности MS Access. Методы противодействия взлому защиты Access.	2			4			Отчет по лабораторной работе
6.2	Архитектура безопасности MS SQL Server. Система безопасности уровня сервера. Аутентификация Windows. Аутентификация SQL Server. Фиксированные роли сервера.	2						Устный опрос
6.3	Система безопасности уровня БД. Фиксированные и пользовательские роли БД. Регистрация пользователей и предоставление им доступа к данным. Администрирование БД в MS SQL Server. Действия при переносе БД на другой компьютер.	2			2			Отчет по лабораторной работе
6.4	Разработка клиент-серверного приложения в VS 2013 с использованием технологии ADO.NET.				8			Отчет по лабораторной работе

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Основная и дополнительная литература

№№ п/п	Список литературы
	Основная
1.	Скакун, В.В. Защита информации в базах данных и экспертных системах: пособие / В.В. Скакун. – Минск: БГУ, 2015. - 135 с.
2.	Змитрович, А.И. Базы данных и знаний: учебное пособие / А.И. Змитрович, В.В. Апанасович, В.В. Скакун. – Минск: Изд. центр БГУ, 2007. – 364 с.
3.	Смирнов, С.Н. Безопасность систем баз данных / С.Н. Смирнов. – М.: Гелиос-АРВ, 2007. – 352с.
4.	Цирлов, В. Л. Основы информационной безопасности. Краткий курс / В. Л. Цирлов. – Феникс, 2008. - 256 с.
5.	Михеева, В. Microsoft Access 2003 / В. Михеева и И. Харитоновна. – СПб: БХВ, 2004. – 1072 с.
6.	Нильсен, Пол . SQL Server 2005. Библия пользователя. Пер с англ./ Пол Нильсен. – Москва, СПб, Киев: Вильямс (Диалектика), 2008. – 1232 с.
	Дополнительная
1.	Мамаев, Е. Microsoft SQL Server 2000. Наиболее полное руководство / Е. Мамаев – СПб: БХВ, 2005. – 1280 с.
2.	Герасименко В.А., Малюк А.А. Основы защиты информации. М.: МИФИ, 2001 г.
3.	Pernul, G. Database Security / G. Pernul // - In: Advances in Computers, Vol. 38. ed. by M. C. Yovits. - Academic Press. – 1994. - pp. 1 - 74.

Перечень тем лабораторных работ:

1.	Организация защиты БД Access на уровне пользователя (4 часа)
2.	Создание БД в консоле MS SQL Server с контролем целостности (4 часа)
3.	Реализация бизнес-логики БД с помощью сохраненных процедур, функций и триггеров (4 часа)
4.	Разработка клиент-серверного приложения с защитой от SQLинъекций (12 часов)
5.	Настройка безопасности и администрирование БД в SQL Server (4 часа)

Методические рекомендации по организации самостоятельной работы студентов

Для выполнения самостоятельной работы студентов, в соответствии с положением о самостоятельной работе студентов, в сетевом доступе размещен комплекс учебных и учебно-методических материалов (программа курса, электронный конспект лекций, методические указания и задания ко всем лабораторным работам, список рекомендуемой литературы и информационных ресурсов и др.).

В распоряжении студентов имеется электронный конспект лекций и примерный проект в VS 2013 для программирования интерфейса к БД MS SQL Server с использованием технологии ADO.NET.

Перечень используемых средств диагностики результатов учебной деятельности студентов

Для оценки уровня знаний студентов используется следующий диагностический инструментарий:

- кратковременные выборочные письменные контрольные на лекциях;
- проверка выполнения лабораторных работ и защита индивидуальных заданий при выполнении лабораторных работ;
- устный зачет.

Рекомендации по контролю качества усвоения знаний и проведению аттестации

В качестве формы итогового контроля по дисциплине используется зачет. Оценка учебных достижений студента на зачете производится в соответствии с постановлением Министерства образования РБ от 29 мая 2012 г. № 23 «Об утверждении Правил проведения аттестации студентов, курсантов, слушателей при освоении содержания образовательных программ высшего образования» и «Положением о рейтинговой системе оценки знаний по дисциплине в Белорусском государственном университете», утвержденным приказом ректора БГУ от 18.08.2015 № 382-ОД.

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ УВО
на _____ / _____ учебный год

№ п/п	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры системного анализа и компьютерного моделирования (протокол № ____ от _____ 20__ г.)

Заведующий кафедрой

(степень, звание)

(подпись)

В.В. Скакун
(И.О.Фамилия)

УТВЕРЖДАЮ
Декан факультета

(степень, звание)

(подпись)

С.В. Малый
(И.О.Фамилия)