Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Хоружий Людмила Ивановна
Должность: Директор института экономики и управления АПК
Дата подписания: 18.07.2023 14:36:55
Уникальный программный ключ:
1e90b132d9b04dce67585160b015dddf2cb1e6a9

УТВЕРЖДАЮ:
Директор Института экономики и управления АПК
_____ Л.И. Хоружий
«17» февраля 2021 г.

Лист актуализации рабочей программы дисциплины
Б1.В.ДВ.04.01 «Безопасность баз данных»

для подготовки экономистов
Специальность: 38.05.01 Экономическая безопасность
Специализация: Экономико-правовое обеспечение экономической безопасности
Форма обучения – очная
Год начала подготовки: 2017

Курс 2
Семестр 4

В рабочую программу вносятся следующие изменения на 2021 год начала подготовки:

1. Заменить таблицу 2 «Распределение трудоёмкости дисциплины по видам работ»

Вид учебной работы	Трудоёмкость	
	час. всего/*	в т.ч. по семестрам
		№ 4
Общая трудоёмкость дисциплины по учебному плану	**72/4**	**72**
1. Контактная работа:	**32,25/4**	**32,25**
Аудиторная работа	**32,25/4**	**32,25**
лекции (Л)	16	16
практические занятия (ПЗ)	16/4	16
контактная работа на промежуточном контроле (КРА)	0,25	0,25
2. Самостоятельная работа (СРС)	**39,75**	**39,75**
самостоятельное изучение разделов, самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к практическим занятиям и т.д.)	30,75	30,75
Подготовка к зачёту (контроль)	9	9
Вид промежуточного контроля:		Зачёт

* в том числе практическая подготовка (см. учебный план)

2. Заменить таблицу 3 «Тематический план учебной дисциплины»

Наименование тем дисциплины	Всего часов на раздел	Аудиторная Работа			Внеаудиторная работа (СРС)
		Л	ПЗ всего/*	ПКР	
Тема 1. Основы информационной безопасности и защиты информации	6	2	-	-	4

Наименование тем дисциплины	Всего часов на раздел	Аудиторная Работа			Внеаудиторная работа (СРС)
		Л	ПЗ всего/*	ПКР	
Тема 2. Законодательный и нормативно-правовой уровни обеспечения информационной безопасности	14	2	4/2	-	8
Тема 3. Программно-технические меры обеспечения информационной безопасности	16	2	4/2	-	10
Тема 4. Основы баз данных	18	6	4	-	8
Тема 5. Средства обеспечения безопасности баз данных	17,75	4	4	-	9,75
Контактная работа на промежуточном контроле (КРА)	0,25	-	-	0,25	-
ИТОГО	**72**	**16**	**16**	**0,25**	**39,75**

* в том числе практическая подготовка (см. учебный план)

3. Заменить таблицу 4 «Содержание лекций, практических занятий и контрольные мероприятия»

№ п/п	№ темы	№ и название лекций/ практических занятий	Формируемые компетенции	Вид контрольного мероприятия	Кол-во часов/ из них практическая подготовка
1.	Тема 1. Основы информационной безопасности и защиты информации	Лекция № 1. Основы информационной безопасности и защиты информации	ПК-28; ПК-33	-	2
2.	Тема 2. Законодательный и нормативно-правовой уровни обеспечения информационной безопасности	Лекция № 2. Организационно-правовые механизмы обеспечения информационной безопасности	ПК-28; ПК-33	-	2
		Практическое занятие № 1. Анализ стандартов. Поиск и анализ законодательных актов по ИБ в справочно-правовой системе КонсультантПлюс. Анализ рисков ИБ.	ПК-28; ПК-33	защита практической работы № 1, устный опрос № 1	4/2
3.	Тема 3. Программно-технические меры обеспечения информационной безопасности	Лекция № 3. Технологии защиты информации. Криптография. Электронная цифровая подпись	ПК-28; ПК-33	-	2
		Практическое занятие № 2. Шифрование. Идентификация и аутентификация. Сетевые сервисы Web 2.0: создание	ПК-28; ПК-33	защита практической работы № 2, устный опрос	4/2

№ п/п	№ темы	№ и название лекций/ практических занятий	Формируемые компетенции	Вид контрольного мероприятия	Кол-во часов/ из них практическая подготовка
		ментальных карт и др.		№ 2	
4.	Тема 4. Основы баз данных	Лекция № 4. СУБД. Модели данных. Этапы проектирования баз данных. Язык запросов SQL.	ПК-28; ПК-33	-	4
		Лекция № 5. Языковые средства управления и обеспечения безопасности данных в реляционных СУБД.	ПК-28; ПК-33	-	2
		Практическое занятие № 3. Создание базы данных и выявление проблем ее безопасности	ПК-28; ПК-33	защита практической работы № 3	4
5.	Тема 5. Средства обеспечения безопасности баз данных	Лекция № 6. Средства обеспечения безопасности баз данных	ПК-28; ПК-33	-	4
		Практическое занятие № 4. Средства идентификации и аутентификации. Средства управления доступом	ПК-28; ПК-33	защита практической работы № 4	4

Разработчики: Лемешко Т.Б., ст. преподаватель _____ «26» 08 2021г.

Худякова Е.В., д.э.н., профессор _____ «26» 08 2021г.

Рабочая программа пересмотрена и одобрена на заседании кафедры прикладной информатики протокол № 1 от «26» августа 2021г.
Заведующий кафедрой _____ Е.В. Худякова

Лист актуализации принят на хранение:
И.о. заведующего выпускающей кафедрой экономической безопасности, анализа и аудита, к.э.н., доцент Т.Н. Гупалова _____ «26» 08 2021 г.

МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ – МСХА имени К.А. ТИМИРЯЗЕВА»
(ФГБОУ ВО РГАУ - МСХА имени К.А. Тимирязева)

Институт экономики и управления АПК
Кафедра прикладной информатики

УТВЕРЖДАЮ:
Директор института
экономики и управления АПК
_____ В.В. Бутырин
«___» _____ 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.В.ДВ.04.01 «Безопасность баз данных»

для подготовки экономистов

ФГОС ВО

Специальность: 38.05.01 Экономическая безопасность
Специализация: «Экономико-правовое обеспечение экономической безопасности»

Курс: 2
Семестр: 4

Форма обучения: очная

Год начала подготовки: 2017

Регистрационный номер _____

Москва, 2020

Разработчик: Лемешко Т.Б., доцент

«26» 08 2019 г.

Рецензент: Остапчук Т.В., к.э.н., доцент

(подпись)

«26» 08 2019 г.

Программа составлена в соответствии с требованиями ФГОС ВО специальности 38.05.01 Экономическая безопасность и учебного плана 2017 года начала подготовки.

Программа обсуждена на заседании кафедры прикладной информатики протокол № 1 от «26» 08 2019 г.

Зав. кафедрой: Худякова Е.В., д.э.н., профессор

(ФИО, ученая степень, ученое звание)

(подпись)

«26» 08 2019 г.

Согласовано:

Председатель учебно-методической комиссии института экономики и управления АПК, Корольков А.Ф., к.э.н., доцент

(ФИО, ученая степень, ученое звание)

(подпись)

«23» 01 2019

Заведующий выпускающей кафедрой экономической безопасности, анализа и аудита Карзаева Н.Н., д.э.н., профессор

(подпись)

«26» 08 2019 г.

Заведующий отделом комплектования ЦНБ

(подпись)

Бумажный экземпляр РПД, копии электронных вариантов РПД и оценочных материалов получены:

Методический отдел УМУ

_____ «__» _____2020 г.

СОДЕРЖАНИЕ

Аннотация
рабочей программы учебной дисциплины
Б1.В.ДВ.04.01 «Безопасность баз данных»
для подготовки экономиста по специальности
38.05.01 Экономическая безопасность, специализации «Экономико-правовое обеспечение экономической безопасности»

Цель освоения дисциплины: формирование знаний об основных положениях теории информационной безопасности и баз данных, умений применять современные методы и средства защиты баз данных.

Место дисциплины в учебном плане: дисциплина включена в вариативную часть дисциплин по выбору учебного плана по специальности 38.05.01 Экономическая безопасность.

Требования к результатам освоения дисциплины: в результате освоения дисциплины формируются следующие компетенции: **ПК-28; ПК-33.**

Краткое содержание дисциплины: Основы информационной безопасности и защиты информации. Законодательный и нормативно-правовой уровни обеспечения информационной безопасности. Административный и процедурный уровни обеспечения информационной безопасности. Основные программно-технические меры обеспечения информационной безопасности. Средства обеспечения защиты информации в системах управления баз данных (СУБД); средства идентификации и аутентификации объектов баз данных, управление доступом; средства контроля целостности информации, организация аудита; типы контроля безопасности: потоковый, контроль вывода, контроль доступа; многоуровневая защита; модели безопасности, применяемые при построении защиты в СУБД; использование транзакции для изолирования действий пользователей; блокировки; ссылочная целостность триггерная и событийная реализации правил безопасности; причины, виды, основные методы нарушения конфиденциальности в СУБД; получение несанкционированного доступа к конфиденциальной информации путем логических выводов; особенности применения криптографических методов; совместное применение средств идентификации и аутентификации, встроенных в СУБД и в ОС; критерии защищенности БД и АИС; технологии удаленного доступа к системам баз данных, тиражирование и синхронизация в распределенных системах баз данных; кластерная организация серверов баз данных; задачи и средства администратора безопасности баз данных.

Общая трудоемкость дисциплины: 72/2 (часы/зач. ед.).

Промежуточный контроль: зачёт в 4-ом семестре.

1. Цель освоения дисциплины

Целью освоения дисциплины «Безопасность баз данных» является формирование знаний об основных положениях теории информационной безопасности и баз данных, умений применять современные методы и средства защиты баз данных.

В результате изучения учебной дисциплины обучающиеся должны:

– знать правовые акты в области защиты информации, основные понятия и угрозы информационной безопасности, основные мероприятия по обеспечению информационной безопасности в профессиональной деятельности;

– знать способы предупреждения, локализации и нейтрализации угроз экономической безопасности.

Полученные умения должны позволить выпускнику:

– ориентироваться в программно-технических, правовых и организационных методах защиты информации;

– использовать методы и средства обеспечения информационной безопасности с целью предотвращения несанкционированного доступа, злоумышленной информации или утраты защищаемой информации;

– оценивать опасность, связанную с угрозами несанкционированного доступа к информации, намеренной модификации данных и утраты служебной информации.

При этом предполагается, что выпускник будет владеть:

– организационно-правовыми методами информационной безопасности;

– навыками моделирования угроз и рисков информационной безопасности;

– современными общими способами обеспечения информационной безопасности;

– базовыми программно-аппаратными методами защиты информации.

Задачи:

1) теоретический компонент: иметь представление о современных концепциях безопасности баз данных; изучить современные способы организации, хранения и доступа к данным; ознакомиться с возможностями современных системам управления базами данных; изучить возможные угрозы на базы данных и способы их предотвращений; ознакомиться с возможностями защиты данных современных системам управления базами данных.

2) познавательный компонент: знать понятие базы данных, уровни представления базы данных в СУБД; математический аппарат реляционной модели данных: реляционная алгебра и реляционное исчисление; этапы проектирования реляционной базы данных; основы структурированного языка запросов SQL; основные средства по обеспечению конфиденциальности данных в базах данных; средства поддержания целостности в базах данных; языковые средства управления доступом к данным.

3) практический компонент: выполнять основные задачи по применению основных команд языка SQL для создания, доступа и модификации базы данных; администрированию защиты сервера баз данных; проектировать и создавать защищенные базы данных; проводить резервное копирование и восстановление базы данных; применять средства аудита для выявления уязвимостей баз данных.

2. Место дисциплины в учебном процессе

Дисциплина «Безопасность баз данных» включена в вариативную часть дисциплин по выбору учебного плана. Дисциплина «Безопасность баз данных»

реализуется в соответствии с требованиями ФГОС ВО, ОПОП ВО и Учебного плана по специальности 38.05.01 Экономическая безопасность.

Предшествующими курсами, на которых непосредственно базируется дисциплина «Безопасность баз данных» являются: «Экономика организации (предприятия)», «Экономическая безопасность», «Управление организацией (предприятием)».

Дисциплина «Безопасность баз данных» является основополагающей для изучения следующих дисциплин: «Информационные системы в экономике», «Моделирование угроз и рисков в экономической безопасности», «Организация и правовое обеспечение информационной безопасности», «Информационные ресурсы в деятельности по обеспечению экономической безопасности», «Организация деятельности службы безопасности предприятий АПК».

Рабочая программа дисциплины «Безопасность баз данных» для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития индивидуальных возможностей и состояния здоровья таких обучающихся.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Изучение данной учебной дисциплины направлено на формирование у обучающихся компетенций, представленных в таблице 1.

Таблица 1

Требования к результатам освоения учебной дисциплины

№ п/п	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны:		
			знать	уметь	владеть
1.	ПК-28	способностью осуществлять сбор, анализ, систематизацию, оценку и интерпретацию данных, необходимых для решения профессиональных задач	Методы и технологии работы с данными, необходимых для решения профессиональных задач	Применять современные системы управления базами данных для анализа, систематизации, интерпретации данных в профессиональной деятельности	Технологиями сбора, анализа и интерпретации данных, необходимых для решения профессиональных задач
2.	ПК-33	способностью анализировать и интерпретировать финансовую, бухгалтерскую и иную информацию, содержащуюся в учетно-отчетной документации, использовать полученные сведения для принятия решений по предупреждению, локализации и нейтрализации угроз экономической безопасности	Особенности финансовой, бухгалтерской и иной информации, содержащейся в учетно-отчетной документации	Использовать современные способы и информационные технологии по предупреждению, локализации и нейтрализации угроз экономической безопасности. Применять средства обеспечения информационной безопасности баз данных	Навыками применения средств обеспечения информационной безопасности баз данных

4. Структура и содержание дисциплины

4.1 Распределение трудоёмкости дисциплины по видам работ по семестрам

Общая трудоёмкость дисциплины составляет 2 зач. единицы (72 часа), их распределение по видам работ в 4 семестре представлено в таблице 2.

Таблица 2

Распределение трудоёмкости дисциплины по видам работ по семестрам

Вид учебной работы	Трудоёмкость	
	час.	в т.ч. по семестрам
		№ 4
Общая трудоёмкость дисциплины по учебному плану	**72**	**72**
1. Контактная работа:	**32,25**	**32,25**
Аудиторная работа	**32,25**	**32,25**
лекции (Л)	16	16
практические занятия (ПЗ)	16	16
контактная работа на промежуточном контроле (КРА)	0,25	0,25
2. Самостоятельная работа (СРС)	**39,75**	**39,75**
самостоятельное изучение разделов, самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к практическим занятиям и т.д.)	30,75	30,75
Подготовка к зачёту (контроль)	9	9
Вид промежуточного контроля:		Зачёт

4.2 Содержание дисциплины

Таблица 3

Тематический план учебной дисциплины

Наименование тем дисциплины	Всего часов на раздел	Аудиторная Работа			Внеаудиторная работа (СРС)
		Л	ПЗ	ПКР	
Тема 1. Основы информационной безопасности и защиты информации	6	2	-	-	4
Тема 2. Законодательный и нормативно-правовой уровни обеспечения информационной безопасности	14	2	4	-	8
Тема 3. Программно-технические меры обеспечения информационной безопасности	16	2	4	-	10
Тема 4. Основы баз данных	18	6	4	-	8
Тема 5. Средства обеспечения безопасности баз данных	17,75	4	4	-	9,75
Контактная работа на промежуточном контроле (КРА)	0,25	-	-	0,25	-
ИТОГО	**72**	**16**	**16**	**0,25**	**39,75**

Тема 1. Основы информационной безопасности и защиты информации

Актуальность проблемы обеспечения безопасности в цифровом обществе. Основные понятия и определения информационной безопасности. Основные составляющие информационной безопасности. Наиболее распространенные угрозы информационной безопасности. Виды мер обеспечения информационной безопасности.

Тема 2. Законодательный и нормативно-правовой уровни обеспечения информационной безопасности

Обзор российского законодательства в области информационной безопасности. Стандарты и спецификации в области информационной безопасности. Морально-этические нормы поведения в цифровом мире. Организационно-правовые механизмы обеспечения информационной безопасности предприятия. Доктрина информационной безопасности РФ, утвержденная Указом Президента РФ от 5.12.2016 г. Закон 149-ФЗ «Об информации…». Закон 1-ФЗ «Об электронной цифровой подписи». Закон 63-ФЗ «Об электронной подписи». Обзор зарубежного законодательства в области информационной безопасности. Сетевые сервисы безопасности по уровням модели OSI. Сетевые механизмы безопасности. Администрирование средств безопасности. Критерии оценки информационной безопасности ISO/IEC 15408. Российское и международное законодательство в области защиты прав на интеллектуальную собственность.

Административный и процедурный уровни обеспечения информационной безопасности. Анализ рисков информационной безопасности. Политика информационной безопасности. Программа работ в области обеспечения информационной безопасности. Основные классы мер процедурного уровня: управление персоналом, физическая защита, поддержание работоспособности, реагирование на нарушения режима безопасности, планирование восстановительных работ.

Тема 3. Программно-технические меры обеспечения информационной безопасности

Основные понятия программно-технического уровня информационной безопасности. Особенности современных информационных систем, существенные с точки зрения безопасности. Технологии защиты данных. Идентификация и аутентификация, управление доступом. Шифрование, контроль целостности. Криптографические алгоритмы. Анализ защищенности. Обеспечение высокой доступности. Сервисы безопасности. Классификация сервисов безопасности с точки зрения места в общей архитектуре мер безопасности. Технологии защиты межсетевого обмена данными. Методы управления средствами сетевой безопасности.

Тема 4. Основы баз данных

Общие принципы построения баз данных. Проектирование инфологической модели базы данных. Метод «Сущность-связь» в нотациях Чена, Баркера, метод IDEF1.X. Проектирование даталогической модели. Функциональные и транзитивные зависимости. Нормализация отношений. Проектирование физической модели данных. Реляционная, иерархическая и сетевая модели; распределенные базы данных в сетях ЭВМ; Файловые системы. Структуры файлов. Именование файлов. Защита файлов. Режим многопользовательского доступа.

Области применения файлов. Общая характеристика, назначение и возможности систем управления базами данных. Основные функции СУБД. Непосредственное управление данными во внешней памяти. Управление буферами оперативной памяти. Управление транзакциями. Журнализация. Поддержка языков БД. Типовая организация современной СУБД. Языковые средства СУБД. Языковые средства манипулирования данными в реляционных СУБД; языковые средства описания данных реляционных СУБД; SEQUEL/SQL СУБД System R. Запросы и операторы манипулирования данными. Операторы определения и манипулирования схемой БД. Определения ограничений целостности и триггеров. Представления базы данных. Особенности языковых средств управления и обеспечения безопасности данных в реляционных СУБД. Определение управляющих структур. Авторизация доступа к отношениям и их полям. Точки сохранения и откаты транзакции. Встроенный SQL. Динамический SQL. Язык SQL в коммерческих реализациях. Стандартизация SQL. Оптимизация производительности и характеристик доступа к базам данных.

Тема 5. Средства обеспечения безопасности баз данных

Средства идентификации и аутентификации объектов баз данных. Языковые средства разграничения доступа, концепция и реализация механизма ролей, организация аудита событий в системах баз данных. Средства контроля целостности информации, организация взаимодействия СУБД и базовой ОС, журнализация, средства создания резервных копии и восстановления баз данных, технологии удаленного доступа к системам баз данных, тиражирование и синхронизация в распределенных системах баз данных. Классификация угроз конфиденциальности СУБД. Причины, виды, основные методы нарушения конфиденциальности. Типы утечки конфиденциальной информации из СУБД, частичное разглашение. Получение несанкционированного доступа к конфиденциальной информации путем логических выводов. Методы противодействия. Особенности применения криптографических методов. Транзакции как средство изолированности пользователей. Сериализация транзакций. Методы сериализации транзакций. Режимы блокировок. Правила согласования блокировок. Двухфазный протокол синхронизационных блокировок. Тупиковые ситуации, их распознавание и разрушение.

4.3 Лекции/практические занятия

Таблица 4

Содержание лекций/ практических занятий и контрольные мероприятия

№ п/п	№ темы	№ и название лекций/ практических занятий	Формируемые компетенции	Вид контрольного мероприятия	Кол-во часов
1.	Тема 1. Основы информационной безопасности и защиты информации	Лекция № 1. Основы информационной безопасности и защиты информации	ПК-28; ПК-33	-	2

№ п/п	№ темы	№ и название лекций/ практических занятий	Формируемые компетенции	Вид контрольного мероприятия	Кол-во часов
2.	Тема 2. Законодательный и нормативно-правовой уровни обеспечения информационной безопасности	Лекция № 2. Организационно-правовые механизмы обеспечения информационной безопасности	ПК-28; ПК-33	-	2
		Практическое занятие № 1. Анализ стандартов. Поиск и анализ законодательных актов по ИБ в справочно-правовой системе КонсультантПлюс. Анализ рисков ИБ.	ПК-28; ПК-33	защита практической работы № 1, устный опрос № 1	4
3.	Тема 3. Программно-технические меры обеспечения информационной безопасности	Лекция № 3. Технологии защиты информации. Криптография. Электронная цифровая подпись	ПК-28; ПК-33	-	2
		Практическое занятие № 2. Шифрование. Идентификация и аутентификация. Сетевые сервисы Web 2.0: создание ментальных карт и др.	ПК-28; ПК-33	защита практической работы № 2, устный опрос № 2	4
4.	Тема 4. Основы баз данных	Лекция № 4. СУБД. Модели данных. Этапы проектирования баз данных. Язык запросов SQL.	ПК-28; ПК-33	-	4
		Лекция № 5. Языковые средства управления и обеспечения безопасности данных в реляционных СУБД.	ПК-28; ПК-33	-	2
		Практическое занятие № 3. Создание базы данных и выявление проблем ее безопасности	ПК-28; ПК-33	защита практической работы № 3	4
5.	Тема 5. Средства обеспечения безопасности баз данных	Лекция № 6. Средства обеспечения безопасности баз данных	ПК-28; ПК-33	-	4
		Практическое занятие № 4. Средства идентификации и аутентификации. Средства управления доступом	ПК-28; ПК-33	защита практической работы № 4	4

Таблица 5

Перечень вопросов для самостоятельного изучения дисциплины

№ п/п	№ темы	Перечень рассматриваемых вопросов для самостоятельного изучения
1.	Тема 1, 2. Основы информационной безопасности и защиты информации. Законодательный и норма-	1. Актуальность проблемы обеспечения безопасности в цифровом обществе, в условиях цифровой экономики и цифровизации сельского хозяйства. 2. Законодательные акты РФ, регулирующие

№ п/п	№ темы	Перечень рассматриваемых вопросов для самостоятельного изучения
	тивно-правовой уровни обеспечения информационной безопасности.	правовые отношения в сфере информационной безопасности и защиты государственной тайны. 3. Морально-этические нормы поведения в цифровом мире. 4. Политика информационной безопасности. Программа работ в области обеспечения информационной безопасности. ПК-28, ПК-33
2.	Тема 3. Программно-технические меры обеспечения информационной безопасности	1. Методы управления средствами сетевой безопасности. 2. Технологии обнаружения вторжений. 3. Инфраструктура защиты на прикладном уровне. 4. Технологии межсетевых экранов. 5. Обеспечение безопасности операционных систем. 6. Технологии аутентификации ПК-28, ПК-33
3.	Тема 4. Основы баз данных	1. Проектирование инфологической модели базы данных. Метод «Сущность-связь» в нотациях Чена, Баркера, метод IDEF1.X. 2. Язык описания данных. Язык манипулирования данными. Язык запросов SELECT (выборка данных). Динамический SQL (генераторы, процедуры, триггеры). Роли и управление доступом средствами SQL. ПК-28, ПК-33
4.	Тема 5. Средства обеспечения безопасности баз данных	1. Методы и средства восстановления системы и базы данных. Резервное копирование и восстановление баз данных. Журнал транзакций. 2. Защита сервера баз данных. Применение средств аудита для выявления уязвимостей в системе безопасности. Аудит уязвимостей СУБД. Средства анализа защищенности. Сканер безопасности. Администрирование сервера баз данных на основе адекватной политики безопасности: работа с учетными записями пользователей, настройка аудита, защита хранимых процедур, анализ стойкости паролей. ПК-28, ПК-33

5. Образовательные технологии

Таблица 6

Применение активных и интерактивных образовательных технологий

№ п/п	Раздел и форма занятия		Наименование используемых активных и интерактивных образовательных технологий
1.	Организационно-правовые механизмы обеспечения информационной безопасности	Л	Интерактивная лекция

№ п/п	Раздел и форма занятия		Наименование используемых активных и интерактивных образовательных технологий
2.	Анализ стандартов. Поиск и анализ законодательных актов по ИБ в справочно-правовой системе КонсультантПлюс. Анализ рисков ИБ.	ПЗ	Групповое обсуждение
3.	СУБД. Модели данных. Этапы проектирования баз данных. Язык запросов SQL.	Л	Интерактивная лекция
4.	Создание базы данных и выявление проблем ее безопасности	ПЗ	Групповое обсуждение
5.	Средства идентификации и аутентификации. Средства управления доступом	ПЗ	Групповое обсуждение

6. Текущий контроль успеваемости и промежуточная аттестация по итогам освоения дисциплины

6.1 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности

1) Примеры заданий практических работ

Пример задания по теме 2: «Законодательный и нормативно-правовой уровни обеспечения информационной безопасности»

Используя информационную систему Консультант Плюс, найти и отобразить с добавлением в раздел «Избранное» и экспортом в Microsoft Word:

1) основные нормативно-правовые акты, регулирующие деятельность в информационной сфере.

2) определения основных категорий информационной безопасности.

3) подборку статей по защите информации.

Примеры заданий по теме 3. «Программно-технические меры обеспечения информационной безопасности»

Пример 1. Используя справочные средства операционной системы Windows найти и отобразить с экспортом в Microsoft Word:

1) понятия учетной записи и домена и типов доступа к операционной системе: глобальные, локальные, ограниченные и административные.

2) описание порядка создания, изменения, активации и удаления учетных записей.

3) основные категории локальных пользователей (пользователи и группы) и конкретных прав каждого вида учетных записей, включая администраторов, пользователей, опытных пользователей, операторов архива, репликаторов и гостей.

Пример 2. Используя средства Internet (kaspersky.ru и т.п.), справочные средства и антивирусное программное обеспечение:

1) найти и отобразить с экспортом в Microsoft Word понятия мошеннического программного обеспечения, хакерских атак, фишинга и спама.

2) найти и отобразить с экспортом в Microsoft Word описание порядка использования и ключевых функций Kaspersky Unlocker и Kaspersky Internet Security, дать сравнительную характеристику ключевых функций Kaspersky Rescue Disk и Kaspersky Antivirus (Kaspersky Virusscanner, Kaspersky Virus Removal Tool и т.д.).

3) открыть антивирусную программу, произвести настройку параметров ее работы, запустить проверку и сформировать отчет о результатах работы.

Пример 3.

1. Зашифровать следующие сообщения методом перестановки:
   ИНФОРМАЦИОННЫЕ СИСТЕМЫ
   ТЕЛЕКОММУНИКАЦИИ.
2. Зашифровать следующие сообщения методом подстановки:
   КОНФИДЕНЦИАЛЬНОСТЬ
   ШИФРОВАНИЕ
   КРИПТОГРАФИЯ
3. Расшифровать следующее сообщение методом перестановки без ключа:
   ЕЫНЬЛАНОСРЕП НАДЕЫН

Пример 4. Используя средства Internet и справочные средства программ резервного копирования найти и отобразить с экспортом в Microsoft Word:

1) понятия полного, дифференциального и инкрементного резервного копирования.

2) описание порядка создания образа и восстановления из него.

3) дать сравнительную характеристику основных функций трех программ резервного копирования по следующим критериям: условия распространения, планирование (работа по расписанию), возможности работы с разделами диска, создания загрузочного диска, шифрования, сжатия, настройки фильтров, онлайн резервного копирования.

Пример 5. Использование сетевых сервисов Веб 2.0.

1. Создание ментальной карты (https:// www.mindmup.com) на тему: «Виды вредоносных программ и методы защиты от них».
2. Создание вебмикса (https:// www.symbaloo.com) для реализации проекта «Интернет: проблемы защиты интеллектуальной собственности».
3. Использование сервиса ленты времени (https:// www.sutori.com) по истории развития компьютерных вирусов.

Примеры заданий по теме 4. «Основы баз данных»

Задания:

1. На сайте Национального открытого Университета «ИНТУИТ» http://www.intuit.ru выбрать 1-2 курса по профилю, например «Базы данных», «Введение в Oracle SQL», «Введение в аналитику больших массивов данных», «Введение в модель данных SQL», пройти обучение и получить Сертификат.

2. Выполнить постановку задачи и разработать информационно-логическую модель предметной области.

1. Представить концептуальную модель БД.

2. Представить логическую модель БД.

3. Представить физическую модель БД

4. Создать базы данных «Учет клиентов туристической фирмы, «Сотрудники» и др.

Примеры заданий по теме 5. Средства обеспечения безопасности баз данных

Задания:

1. Средства идентификации и аутентификации в СУБД MS SQL Server

Вся работа выполняется с помощью языка Transact-SQL!

1. Для доступа к SQL Server создайте 4 учетные записи (логины): *«Администратор БД», «Сотрудник отдела кадров», «Сотрудник отдела продаж», «Сотрудник отдела поставок»*;

2. Учетную запись «Администратор» наделите привилегиями системного администратора (с помощью системной роли);

3. Напишите SQL-скрипты для получения следующей информации:

3.1. Секретный идентификатор, имя, хэш пароля определенной учетной записи;

3.2. Список всех учетных записей сервера;

3.3. Список всех учетных записей сервера, обладающих правами администратора.

4. Напишите SQL-скрипты для выполнения следующих действий с учетной записью SQL-сервера:

4.1. Блокировка учетной записи (временное приостановление действия);

4.2. Разблокировка учетной записи;

4.3. Изменение пароля учетной записи;

4.4. Изменение БД по умолчанию;

4.5. Удаление учетной записи.

5. Напишите SQL-скрипты для выполнения следующих действий с учетной записью операционной системы (ОС):
5.1. Регистрация учетной записи ОС в качестве учетной записи в MS SQL Server;

5.2. Отмена регистрации учетной записи ОС в качестве учетной записи в MS SQL Server;

5.3. Запрет подключений учетной записи ОС в качестве учетной записи в MS SQL Server.
6. Для каждой учетной записи, созданной в 1 пункте, кроме «Администратор БД» добавьте пользователя в вашу БД (AdventureWorks2008R2).

2. Средства управления доступом

1. Используя роли и привилегии каждому пользователю определите следующие права:

1.1. *«Сотрудник отдела продаж» –*

a. разрешение на добавление, изменение, удаление данных о сотрудниках компании Adventure Works Cycles;

b. запрет на просмотр, изменение и удаление данных продукции, продаж и поставок.

1.2. *«Сотрудник отдела продаж» –*

a. разрешение на добавление, изменение, удаление данных о заказчиках и продажах;

b. разрешение на просмотр данных о продукции, поставщиках и поставках;

c. запрет на изменение и удаление данных о продукции, поставщиках и поставках

1.3. *«Сотрудник отдела поставок»*

a. разрешение на добавление, изменение, удаление данных о поставщиках и поставках;

b. разрешение на изменение информации о количестве продукции на складе компании;

c. для данных о продукции - разрешение на просмотр и запрет на изменение и удаление;

d. запрет на просмотр, изменение и удаление данных о сотрудниках и продажах.

2. Напишите SQL-скрипты для получения следующей информации:

2.1. Все пользователи и все привилегии текущей БД;

2.2. Список всех ролей и пользователей, которым присвоены эти роли;

2.3. Список всех ролей, назначенных текущему пользователю;

2.4. Список привилегий, ассоциированных с какой-то конкретной ролью;

2.5. Список всех привилегий текущего пользователя.

Напишите код запроса с использованием конструкции EXECUTE AS, в ходе которого «Сотрудник отдела поставок» смог бы выполнять запросы от имени пользователя «Сотрудник отдела продаж».

2) Вопросы для устного опроса

Устный опрос № 1.

Тема 1. Основы информационной безопасности и защиты информации

Тема 2. Законодательный и нормативно-правовой уровни обеспечения информационной безопасности

1. Понятие информационной безопасности
2. Субъекты и объекты информационной безопасности
3. Понятие и функции системы защиты информации
4. Общие принципы обеспечения информационной безопасности
5. Специальные принципы обеспечения информационной безопасности
6. Обеспечивающие подсистемы защиты информации
7. Нормативно-правовые основы информационной безопасности
   1. Понятие информационной угрозы
   2. Причины реализации информационных угроз
   3. Виды реализации угроз информационной безопасности
   4. Классификация информационных угроз
   5. Способы воздействия информационных угроз
8. Прогресс информационных технологий и необходимость обеспечения
9. безопасности
10. Основные понятия информатизации общества и информационной безопасности
11. Структура понятия «Информационная безопасность»
12. Субъекты и объекты информационной безопасности
13. Нормативно-правовое регулирование информационной безопасности
14. Стандарты и спецификации в области информационной безопасности.
15. Типы международных организаций в сфере информационной безопасности
16. Направления работы крупных альянсов в сфере информационной безопасности
17. Понятие и особенности экономической информации как объекта безопасности
18. Перечень сведений, относящихся к коммерческой тайне
19. Перечень сведений, которые не могут составлять коммерческую тайну

20. Объекты банковской тайны
21. Статьи Уголовного кодекса о компьютерных преступлениях
22. Доктрина информационной безопасности РФ
23. Федеральный закон от №149-ФЗ «Об информации, информационных технологиях и о защите информации»
24. Федеральный закон от №63-ФЗ «Об электронной подписи»
25. 16. Принципиальные подходы к обеспечению информационной безопасности
26. Сравнительная характеристика фрагментного и комплексного подхода к защите
27. информации
28. Общие принципы обеспечения информационной безопасности
29. Специфические методы обеспечения информационной безопасности
30. Принципы построения системы информационной безопасности
31. Системный подход к защите информации
32. Требования к системе мер защиты информации
33. Принципы построения и особенности практической реализации системы защиты информации экономического субъекта
34. Механизм обеспечения информационной безопасности РФ в сфере экономики
35. Цели, задачи и функции системы защиты информации
36. Обеспечивающие компоненты системы защиты информации
37. Методы и средства обеспечения информационной безопасности
38. Российское и международное законодательство в области защиты прав на интеллектуальную собственность.
39. Анализ рисков информационной безопасности.

Устный опрос № 2.

Тема 3. Программно-технические меры обеспечения информационной безопасности

1. Классификация вредоносного программного обеспечения
2. Классификация компьютерных преступлений
3. Методы обеспечения информационной безопасности
4. Средства обеспечения информационной безопасности
5. Криптографическое обеспечение информационной безопасности
6. Организационное обеспечение информационной безопасности
7. Особенности и этапы построения системы защиты информации
8. Методы реализации механизмов защиты информации
9. План построения системы защиты информации
10. Функции службы информационной безопасности
11. Симметричные криптосистемы. AES. ГОСТ
12. Ассиметричные криптосистемы. RSA. El Gamal
13. Криптографические протоколы. Общие понятия, типы криптопротоколов

14. Протоколы аутентификации. Слабости парольных протоколов аутентификации. Виды атак и угроз для протоколов аутентификации. Полнота, корректность. Стойкость протокола
15. Протокол аутентификации Фейге – Фиата - Шамира. Анализ протокола.
16. Протокол аутентификации Шнорра. Анализ протокола. Рекомендации по использованию. Сфера применения протокола
17. Протоколы электронной подписи. Общие понятия и определения. Виды атак и угроз для протоколов электронной подписи. Стойкость протокола
18. Криптографические хэш-функции. Определение и требования к ним. Задача вычисления коллизий хэш-функций. Атаки и угрозы для хэш-функций, стойкость хэш-функции. Области применения хэш-функций
19. Хэш-функция SHA. Построение хэш-функций на основе стойких криптосистем
20. Использование хэш-функций в протоколах электронной подписи. Протокол электронной подписи DSS
21. Электронная подпись в системе RSA.
22. Архитектура системы безопасности ОС Windows.
23. Архитектура системы безопасности ОС Windows
24. Субъект доступа
25. Объект доступа
26. Механизм контроля доступа
27. Диспетчер учётных записей SAM. Пароли и ключи пользователей
28. База учётных записей SAM: типичные атаки и методы её защиты
29. Введение в файловую систему NTFS. Права доступа стандартные, специфичные и родовые
30. Разрешения NTFS индивидуальные, стандартные и специальные
31. Механизм наследования разрешений. Средства редактирования разрешения NTFS
32. Шифрование данных в NTFS. Рекомендации по защите средствами NTFS
33. Безопасность сервера SMB. Введение в протокол SMB
34. Типичные атаки на протокол и методы защиты. Аудит сервера SMB
35. Проверка подлинности при входе в домен Windows
36. Защита реестра Windows
37. Безопасность серверов RAS и IIS
38. Инфраструктура открытых ключей PKI
39. Протокол KERBEROS
40. Криптоинтерфейс, криптопровайдеры
41. Защищенные протоколы и защищенные компьютерные системы
42. Удаленные атаки на защищенные компьютерные системы и методы защиты от них

3) Перечень вопросов, выносимых на промежуточную аттестацию (зачет)

1. Прогресс информационных технологий и необходимость обеспечения безопасности
2. Основные понятия информатизации общества и информационной безопасности
3. Структура понятия «Информационная безопасность»
4. Субъекты и объекты информационной безопасности
5. Нормативно-правовое регулирование информационной безопасности
6. Типы международных организаций в сфере информационной безопасности
7. Направления работы крупных альянсов в сфере информационной безопасности
8. Понятие и особенности экономической информации как объекта безопасности
9. Перечень сведений, относящихся к коммерческой тайне
10. Перечень сведений, которые не могут составлять коммерческую тайну
11. Объекты банковской тайны
12. Статьи Уголовного кодекса о компьютерных преступлениях
13. Доктрина информационной безопасности РФ
14. Федеральный закон от №149-ФЗ «Об информации, информационных технологиях и о защите информации»
15. Федеральный закон от №63-ФЗ «Об электронной подписи»
16. Принципиальные подходы к обеспечению информационной безопасности
17. Сравнительная характеристика фрагментного и комплексного подхода к защите информации
18. Общие принципы обеспечения информационной безопасности
19. Специфические методы обеспечения информационной безопасности
20. Принципы построения системы информационной безопасности
21. Системный подход к защите информации
22. Требования к системе мер защиты информации
23. Принципы построения и особенности практической реализации системы защиты информации экономического субъекта
24. Механизм обеспечения информационной безопасности РФ в сфере экономики
25. Цели, задачи и функции системы защиты информации
26. Защиты от несанкционированного доступа. Идентификация и аутентификация пользователя.
27. Защита интеллектуальной собственности средствами патентного и авторского права.
28. Программно-аппаратные средства обеспечения информационной безопасности в информационных сетях.
29. Симметричные шифры.
30. Ассиметричные шифры.
31. Криптографические протоколы.
32. Криптографические хеш-функции.

33. Электронная подпись.
34. Организационное обеспечение информационной безопасности.
35. Служба безопасности организации.
36. Обеспечивающие компоненты системы защиты информации
37. Методы и средства обеспечения информационной безопасности
38. Сущность криптографических методов
39. Организационно-административные мероприятия обеспечения компьютерной безопасности
40. Принципы обеспечения информационной безопасности на основе инженерно-технического обеспечения
41. Меры предупреждения и защиты от компьютерных преступлений
42. Информационные угрозы и их классификация
43. Действия и события, нарушающие информационную безопасность
44. Основные виды каналов утечки информации
45. Пути несанкционированного доступа к информации
46. Стратегия и тактика злоумышленника при несанкционированном доступе
47. Личностно - профессиональные характеристики сотрудников, способствующие реализации информационных угроз
48. Способы воздействия угроз на информационные объекты
49. Вредоносные программы, их виды
50. Признаки воздействия вирусов на компьютерную систему
51. Исторические аспекты компьютерных преступлений
52. Уголовно-правовая характеристика компьютерных преступлений,
53. Компьютерные преступления и их классификация
54. Субъекты компьютерных преступлений
55. Объективная сторона компьютерных преступлений
56. Уголовно-правовой контроль над компьютерной преступностью в РФ
57. Организация системы защиты информации экономических систем
58. Этапы построения системы защиты информации
59. Политика информационной безопасности
60. Способы практической реализации механизмов защиты информации
61. План построения системы защиты информации
62. Организация конфиденциального делопроизводства
63. Структура и функции службы информационной безопасности компании
64. Типы политики информационной безопасности
65. Оценка эффективности инвестиций в информационную безопасность
66. Обеспечение информационной безопасности автоматизированных банковских систем
67. Информационная безопасность электронной коммерции
68. Обеспечение компьютерной безопасности учетной информации
69. Информационная безопасность предпринимательской деятельности
70. Методика защиты электронной почты
71. Обеспечение информационной безопасности должностных лиц и представителей деловых кругов
72. Электронная цифровая подпись и особенности ее применения
73. Защита информации в Интернете

74. Информационная безопасность пользователей мобильных устройств

75. Понятие безопасности БД. Угрозы безопасности БД: общие и специфичные.

76. Понятие политики безопасности. Сущность политики безопасности. Цели формализации политики безопасности. Принципы построения защищенных систем.

77. Дискреционные модели безопасности СУБД. Реализация ролевой модели политики безопасности в СУБД Oracle.

78. Мандатная модель политики безопасности.

79. БД с многоуровневой секретностью (MLS). Многозначность. Реализация модели MLS. Авторизация меток пользователя. Специальные привилегии доступа. Меточные функции. Опции ограничения.

80. Метаданные и словарь данных. Назначение словаря данных. Доступ к словарю данных. Состав словаря. Представления словаря.

81. Понятие транзакции. Фиксация транзакции. Прокрутки вперед и назад. Контрольная точка. Откат. Транзакции как средство изолированности пользователей. Сериализация транзакций.

82. Блокировки. Режимы блокирования. Правила согласования блокировок. Двухфазный протокол синхронизационных блокировок. Взаимоблокировки, их распознавание и разрушение.

83. Целостность кода приложения. SQL-инъекции. Динамическое выполнение кода SQL и PL/SQL. Категории атак SQL-инъекцией. Методы SQL-инъекций. Противодействие атакам типа SQL-инъекции.

84. Подотчетность действий пользователя и аудит связанных с безопасностью событий. Регистрация действий пользователя. Управление набором регистрируемых событий. Анализ регистрационной информации.

85. Типовая организация СУБД.

86. Основные функции СУБД

87. Непосредственное управление данными во внешней памяти

88. Управление буферами оперативной памяти

89. Управление транзакциями

90. Журнализация

91. Поддержка языков БД

92. Системы, основанные на инвертированных списках, иерархические и сетевые СУБД.

93. Структуры данных

94. Манипулирование данными

95. Ограничения целостности

96. Базовые понятия реляционных баз данных

97. Реляционная модель данных

98. Целостность сущности и ссылок

99. Реляционная алгебра

100. Реляционное исчисление

101. Проектирование реляционных баз данных с использованием нормализации

102. Семантические модели данных

103. Внутренняя организация реляционных СУБД
104. Структуры внешней памяти, методы организации индексов
105. Транзакции и целостность баз данных
106. Изолированность пользователей
107. Особенности языковых средств управления и обеспечения безопасности данных в реляционных СУБД
108. Оптимизация производительности и характеристик доступа к базам данных
109. Средства идентификации и аутентификации объектов баз данных
110. Языковые средства разграничения доступа, концепция и реализация механизма ролей, организация аудита событий в системах баз данных
111. Средства контроля целостности информации
112. Организация взаимодействия СУБД и базовой ОС
113. Журнализация, средства создания резервных копии и восстановления баз данных, технологии удаленного доступа к системам баз данных
114. Тиражирование и синхронизация в распределенных системах баз данных
115. Задачи и средства администратора безопасности баз данных
116. Язык реляционных баз данных SQL
117. Запросы и операторы манипулирования данными
118. Операторы определения и манипулирования схемой БД
119. Определения ограничений целостности и триггеров
120. Представления базы данных
121. Определение управляющих структур
122. Авторизация доступа к отношениям и их полям
123. Точки сохранения и откаты транзакции
124. Встроенный SQL
125. Динамический SQL
126. Стандартизация SQL
127. Использование SQL при прикладном программировании
128. Компиляторы SQL. Проблемы оптимизации
129. Общая схема обработки запроса
130. СУБД в архитектуре "клиент-сервер"
131. Архитектура "клиент-сервер"
132. Распределенные базы данных
133. Разновидности распределенных систем
134. Объектно-ориентированные модели данных
135. Языки программирования объектно-ориентированных баз данных
136. Языки запросов объектно-ориентированных баз данных
137. Ненавигационные языки запросов
138. Примеры объектно-ориентированных СУБД

6.2 Описание показателей и критериев контроля успеваемости, описание шкал оценивания

Для оценки знаний, умений, навыков и формирования компетенций по дисциплине применяется традиционная система контроля и оценки успеваемости студентов.

При использовании традиционной системы контроля и оценки успеваемости студентов представлены критерии выставления оценок: «зачтено», «не зачтено».

Промежуточный контроль знаний проводится в форме зачета.

Критерии оценки зачёта представлены в таблице 7.

Таблица 7

Критерии выставления оценок на зачете

Оценка	Критерии оценивания
Зачтено	**«Зачтено»** выставляется, если студент самостоятельно и полностью использует возможности программных средств для решения прикладных задач; самостоятельно подтверждает ответ конкретными примерами; правильно и обстоятельно отвечает на дополнительные вопросы преподавателя; умеет пользоваться справочной литературой, поиском информации, раздаточным материалом.
Не зачтено	**«Не зачтено»** выставляется, если студент не может использовать программные средства при решении задач; не может подтвердить ответ конкретными примерами; не отвечает на большую часть дополнительных вопросов преподавателя; не может самостоятельно использовать справочную литературу, раздаточный материал, поиск информации.

7. Учебно-методическое и информационное обеспечение дисциплины

7.1 Основная литература

1. Петров, С.В. Информационная безопасность: учебное пособие / С. В. Петров. – Новосибирск – М.: Арта, 2012. – 294 с.

2. Волк, В. К. Базы данных. Проектирование, программирование, управление и администрирование: учебник / В. К. Волк. – Санкт-Петербург: Лань, 2020. – 244 с. – ISBN 978-5-8114-4189-1. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/126933 (открытый доступ).

3. Нестеров, С. А. Основы информационной безопасности: учебное пособие / С. А. Нестеров. – 5-е изд., стер. – Санкт-Петербург: Лань, 2019. – 324 с. – ISBN

978-5-8114-4067-2. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/114688 (открытый доступ).

7.2 Дополнительная литература

1. Бабенко, Л.К., Басан, А.С., Журкин, И.Г., Макаревич, О.Б. Защита данных геоинформационных систем/ Л.К. Бабенко, А.С. Басан, И.Г. Журкин, О.Б. Макаревич. – М.: Гелиос АРВ, 2010. – 336 с.

2. Карпычев, В.Ю. Техническая защита информации. Каналы утечки информации: учебное пособие/ В.Ю. Карпычев, М. А. Степаненко, О. П. Тимофеева. – Нижний Новгород, 2018. – 92 с.

3. Гилязова, Р. Н. Информационная безопасность. Лабораторный практикум: учебное пособие / Р. Н. Гилязова. – Санкт-Петербург: Лань, 2020. – 44 с. – ISBN 978-5-8114-4294-2. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/130179 (открытый доступ).

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Бесплатное дистанционное обучение в Национальном Открытом Университете «ИНТУИТ» [Электронный ресурс]. – Режим доступа: http://www.intuit.ru (открытый доступ).

2. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс]/ Шаньгин В.Ф. – Электрон. Текстовые данные. – Саратов: Профобразование, 2017. – 544 с. – Режим доступа: http://www.iprbookshop.ru/63592.html (открытый доступ)

9. Перечень программного обеспечения и информационных справочных систем

1. Справочная правовая система «КонсультантПлюс» (открытый доступ): [Электронный ресурс]. – Режим доступа: www.consultant.ru. – Загл. с экрана.

Таблица 8

Перечень программного обеспечения

Наименование темы учебной дисциплины	Наименование программы	Тип программы	Автор	Год разработки
По всем темам	Microsoft Windows 7 и	Операционная	Microsoft	2009

дисциплины	выше	система		
	Microsoft Office 2010 и выше, Microsoft SQL Server	Пакет офисных программ, СУБД		2010
	Google Chrome	Браузер		2012

10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для проведения лекционных и практических занятий по дисциплине «Безопасность баз данных» необходимы аудитория и компьютерный класс, подключенные к сети Интернет, оснащенные средствами мультимедиа и программными средствами: MS Windows 7/8/10; MS Office 2007/2010/2013/365 (Office Online), Microsoft SQL Server, системой КонсультантПлюс, программой демонстрации NetOp School, браузером Google Chrome.

Лекции проводятся в специализированной аудитории, оборудованной мультимедийным проектором для демонстрации компьютерных презентаций.

Для проведения практических занятий по дисциплине «Безопасность баз данных» необходим компьютерный класс с установленными на ПК программным обеспечением, указанным в п. 9.

Таблица 9

Сведения об обеспеченности специализированными аудиториями, кабинетами, лабораториями

Наименование специальных помещений и помещений для самостоятельной работы (№ учебного корпуса, № аудитории)	**Оснащенность специальных помещений и помещений для самостоятельной работы**
1	2
Аудитория для проведения занятий лекционного типа № 118 - уч. корпус № 15	Видеопроектор 3500 Лм
Аудитория для проведения практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации №УИТ-113, уч. корпус №15	Персональные компьютеры в количестве 20 штук
Аудитория для проведения практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации №УИТ-110, уч. корпус №15	Персональные компьютеры в количестве 20 штук
Аудитория для проведения практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации №УИТ-114, уч. корпус №15	Персональные компьютеры (терминалы) в количестве 20 штук
Аудитория для проведения практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежу-	Персональные компьютеры (терминалы) в количестве 20 штук

Наименование специальных помещений и помещений для самостоятельной работы (№ учебного корпуса, № аудитории)	Оснащенность специальных помещений и помещений для самостоятельной работы
1	2
точной аттестации №УИТ-102, уч. корпус №15	
Центральная научная библиотека имени Н.И. Железнова	Читальные залы библиотеки
Общежитие	Комната для самоподготовки

11. Методические рекомендации студентам по освоению дисциплины

Изучение учебной дисциплины «Безопасность баз данных» включает освоение материалов лекций, приобретение практических навыков работы с программными средствами.

На лекциях при помощи мультимедиа проектора и презентаций раскрываются основные теоретические вопросы дисциплины, делаются акценты на наиболее сложные положения изучаемого материала.

Лекционный материал следует просматривать и изучать по конспекту/электронной презентации самостоятельно после аудиторных занятий. Для более углубленного изучения материала необходимо использовать рекомендованную литературу и Интернет-ресурсы.

Практические занятия проводятся в компьютерных классах с применением методических материалов. На занятиях необходимо иметь электронный носитель информации – флэш-карту для сохранения результатов своей работы. Учебные материалы можно сохранять в облачных сервисах: Google Диск, Яндекс.Диск, Облако Mail.Ru, Dropbox.

Посещение лекций и практических занятий – обязательно.

Консультирование по выполнению заданий проводится в компьютерных классах во время консультаций по графику (см. на стендах кафедры), а также через электронный обмен сообщениями с преподавателями, посредством Интернет и электронной информационно-образовательной среды Университета через личный кабинет.

Необходимо соблюдать сроки выполнения всех заданий.

Полученные оценки за выполненные задания являются основой для промежуточной аттестации.

Виды и формы отработки пропущенных занятий

Студент, обязан отработать:

– пропущенные лекции – представив преподавателю конспект лекции, ответив на вопросы устно;

– пропущенные практические занятия – в форме выполнения заданий, устного опроса, посещения дополнительных занятий.

12. Методические рекомендации преподавателям по организации обучения по дисциплине

Учебный процесс по курсу «Безопасность баз данных» включает следующие организационные формы: лекции, практические занятия и консультации, а также систему контроля знаний, самостоятельную работу студентов.

Методика чтения лекций зависит от цели и задач изучения предмета/раздела, а также уровня общей подготовки обучающихся, форма ее проведения – от характера темы и содержания материала. Высокая эффективность деятельности преподавателя во время чтения лекции достигается за счет глубокого освоения предметной области, педагогического мастерства, высокой речевой культуры и ораторского искусства, когда учитывается психология аудитории, закономерности восприятия, внимания, мышления, эмоциональные процессы учащихся, обратная связь и принципы дидактики.

При подготовке материала лекции преподавателю необходимо:

– учитывать требования государственного образовательного стандарта, учебного плана и рабочей программы;

– применять принципы дидактики (наглядность, от теории к практике, доступность, структуризация и систематизация и т.д.);

– уметь создавать интерактивные презентации;

– уметь использовать технические (проектор) и программные средства (например, программу подготовки презентаций MS PowerPoint, программу управления компьютерным классом NetOp School) и др.

Для проведения практических занятий преподавателю следует разрабатывать задания различной степени сложности, инструкции (методические указания) по выполнению каждого задания, раздаточный материал в печатном и электронном виде.

По курсу «Безопасность баз данных» должны быть организованы:

– «очные» консультации в компьютерном классе, проводимые преподавателем согласно графику (размещается на стендах кафедры);

– off-line консультации, проводимые преподавателем с помощью электронной почты;

– взаимодействия в электронной информационно-образовательной среде Университета через личный кабинет.

Для организации контрольных мероприятий преподавателю следует подготовить вопросы для устного опроса и практические задания. Преподаватель должен использовать различные методы обучения:

– объяснительно-иллюстративный (лекция, объяснение, работа с учебником, демонстрация презентаций);

– репродуктивный (воспроизведение действий по применению знаний на практике, деятельность по алгоритму, программирование);

– частично-поисковый (поиск решения познавательных задач под руководством преподавателя);

– исследовательский метод, в котором после анализа материала, постановки проблем и задач и краткого устного или письменного инструктажа обу-

чаемые самостоятельно изучают литературу, источники, ведут наблюдения и измерения и выполняют другие действия поискового характера.

- активные методы: групповое обсуждение и др.

Программу разработала:

Лемешко Т.Б., доцент _____

РЕЦЕНЗИЯ

на рабочую программу дисциплины
Б1.В.ДВ.04.01 «Безопасность баз данных»
ОПОП ВО по специальности 38.05.01 Экономическая безопасность, специализации «Экономико-правовое обеспечение экономической безопасности»
(квалификация выпускника – бакалавр)

Остапчук Татьяной Владимировной, доцентом кафедры бухгалтерского учета ФГБОУ ВО РГАУ-МСХА имени К.А. Тимирязева, кандидатом экономических наук (далее по тексту рецензент) проведено рецензирование рабочей программы учебной дисциплины «Безопасность баз данных» по специальности 38.05.01 Экономическая безопасность, специализации «Экономико-правовое обеспечение экономической безопасности», разработанной в ФГБОУ ВО «Российский государственный аграрный университет – МСХА имени К.А. Тимирязева» на кафедре прикладной информатики (разработчик – Лемешко Т.Б., доцент).

Рассмотрев представленные на рецензирование материалы, рецензент пришел к следующим выводам:

1. Предъявленная рабочая программа дисциплины «Безопасность баз данных» (далее по тексту Программа) *соответствует* требованиям ФГОС ВО по специальности 38.05.01 Экономическая безопасность. Программа *содержит* все основные разделы, *соответствует* требованиям к нормативно-методическим документам.

2. Представленная в Программе ***актуальность*** учебной дисциплины в рамках реализации ОПОП ВО *не подлежит сомнению* – дисциплина относится к вариативной части дисциплин по выбору учебного цикла – Б1.В.ДВ

3. Представленные в Программе ***цели*** дисциплины *соответствуют* требованиям ФГОС ВО специальности 38.05.01 Экономическая безопасность.

4. В соответствии с Программой за дисциплиной «Безопасность баз данных» закреплены 2 профессиональных ***компетенции***. Дисциплина «Безопасность баз данных» и представленная Программа *способна реализовать* их в объявленных требованиях.

5. ***Результаты обучения***, представленные в Программе в категориях знать, уметь, владеть *соответствуют* специфике и содержанию дисциплины и *демонстрируют возможность* получения заявленных результатов.

6. Общая трудоёмкость дисциплины «Безопасность баз данных» составляет 2 зачётных единицы (72 часа).

7. Информация о взаимосвязи изучаемых дисциплин и вопросам исключения дублирования в содержании дисциплин *соответствует* действительности. Дисциплина «Безопасность баз данных» взаимосвязана с другими дисциплинами ОПОП ВО и Учебного плана по специальности 38.05.01 Экономическая безопасность**.**

8. Представленная Программа предполагает использование современных образовательных технологий, используемые при реализации различных видов учебной работы. Формы образовательных технологий *соответствуют* специфике дисциплины.

9. Программа дисциплины «Безопасность баз данных» предполагает проведение занятий в интерактивной форме.

10. Виды, содержание и трудоёмкость самостоятельной работы студентов, представленные в Программе, *соответствуют* требованиям к подготовке выпускников, содержащимся во ФГОС ВО специальности 38.05.01 Экономическая безопасность.

11. Представленные и описанные в Программе формы *текущей* оценки знаний *соответствуют* специфике дисциплины и требованиям к выпускникам.

Форма промежуточного контроля знаний студентов, предусмотренная Программой, осуществляется в форме зачёта, что *соответствует* статусу дисциплины, как дисциплины по выбору вариативной части учебного цикла – Б1.В.ДВ ФГОС ВО специальности 38.05.01 Экономическая безопасность.

12. Формы оценки знаний, представленные в Программе, *соответствуют* специфике дисциплины и требованиям к выпускникам.

13. Учебно-методическое обеспечение дисциплины представлено: основной литературой – 3 источника, дополнительной литературой – 3 наименования, Интернет-ресурсы – 2 источника и *соответствует* требованиям ФГОС ВО специальности 38.05.01 Экономическая безопасность.

14. Материально-техническое обеспечение дисциплины соответствует специфике дисциплины «Безопасность баз данных» и обеспечивает использование современных образовательных, в том числе интерактивных методов обучения.

15. Методические рекомендации студентам и методические рекомендации преподавателям по организации обучения по дисциплине дают представление о специфике обучения по дисциплине «Безопасность баз данных».

ОБЩИЕ ВЫВОДЫ

На основании проведенного рецензирования можно сделать заключение, что характер, структура и содержание рабочей программы дисциплины «Безопасность баз данных» ОПОП ВО по специальности 38.05.01 Экономическая безопасность, специализации «Экономико-правовое обеспечение экономической безопасности» (квалификация выпускника – экономист), разработанной Лемешко Т.Б., доцентом кафедры прикладной информатики, соответствует требованиям ФГОС ВО, современным требованиям экономики, рынка труда и позволит при её реализации успешно обеспечить формирование заявленных компетенций.

Рецензент: Остапчук Т.В., доцент кафедры бухгалтерского учета ФГБОУ ВО РГАУ-МСХА имени К.А. Тимирязева, кандидат экономических наук

_____ «20» 08 2019 г.
(подпись)