МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

УТВЕРЖДАЮ
Директор ИЭиАС
_____ С.И. Лукьянов

26.02.2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

БЕЗОПАСНОСТЬ СИСТЕМ БАЗ ДАННЫХ

Направление подготовки (специальность)
10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ
Направленность (профиль/специализация) программы
10.05.03 специализация N 7 "Обеспечение информационной безопасности распределенных информационных систем";

Уровень высшего образования - специалитет

Форма обучения
очная

Институт/ факультет	Институт энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	3
Семестр	5, 6

Магнитогорск
2020 год

Рабочая программа составлена на основе ФГОС ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем (приказ Минобрнауки России от 01.12.2016 г. № 1509)

Рабочая программа рассмотрена и одобрена на заседании кафедры Информатики и информационной безопасности
18.02.2020, протокол № 6

Зав. кафедрой _____ И.И. Баранкова

Рабочая программа одобрена методической комиссией ИЭиАС
26.02.2020 г. протокол № 5

Председатель _____ С.И. Лукьянов

Рабочая программа составлена:
доцент кафедры ИиИБ, канд. техн. наук _____ У.В. Михайлова

Рецензент:
Начальник отдела информационной безопасности АО "КУБ",

_____ М.М. Близнецов

Лист актуализации рабочей программы

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2020 - 2021 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от 1 сентября 2020 г. № 1
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2021 - 2022 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2022 - 2023 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2023 - 2024 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2024 - 2025 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

1 Цели освоения дисциплины (модуля)

Целью дисциплины «Безопасность систем баз данных» является изучение реализации политики безопасности баз данных и формирование у обучающихся навыков ее практического применения в соответствии с требованиями ФГОС ВО по специальности «Информационная безопасность автоматизированных систем». Дисциплина «Безопасность систем баз данных» рассматривает основные принципы и основные направления обеспечения безопасности данных.

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Безопасность систем баз данных входит в базовую часть учебного плана образовательной программы.

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:

Организация ЭВМ и вычислительных систем

Введение в специальность

Языки программирования

Сети и системы передачи информации

Основы информационной безопасности

Информационные технологии. Базы данных

Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:

Технология построения защищенных распределенных приложений

Информационная безопасность распределенных информационных систем

Тестирование систем защиты информации автоматизированных систем

Защита электронного документооборота

Методы мониторинга информационной безопасности АС

Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности

Управление информационной безопасностью

Информационная безопасность систем организационного управления

Научно-исследовательская работа

3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения

В результате освоения дисциплины (модуля) «Безопасность систем баз данных» обучающийся должен обладать следующими компетенциями:

Структурный элемент компетенции	Планируемые результаты обучения
ПК-23 способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	

Знать	Методы формирования требований по защите информации, обрабатываемой в СУБД. Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации, обрабатываемой в СУБД. Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем. Организационные меры по защите информации, обрабатываемой в СУБД.
Уметь	Использовать методы формирования требований по защите информации, обрабатываемой в СУБД. Классифицировать средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации, обрабатываемой в СУБД. Организовывать безопасность АРМ, на которых установлена СУБД.
Владеть	Методами формирования требований по защите информации, обрабатываемой в СУБД. Навыками анализа методов формирования требований по защите информации, обрабатываемой в СУБД.
ПК-25 способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций	
Знать	Принципы работы баз данных. Основные средства обеспечения безопасности данных. Принципы администрирования баз данных. Средства обеспечения безопасности данных. Организацию защиты информации баз данных. Сравнительный анализ эффективности применения средств обеспечения безопасности данных.
Уметь	Анализировать работоспособность базы данных. Принимать участие в настройке средств обеспечения безопасности данных, обрабатываемых в СУБД. Самостоятельно применять средства обеспечения безопасности данных. Участвовать в восстановлении работоспособности систем баз данных при возникновении нештатных ситуаций. Организовывать безопасность систем баз данных.
Владеть	Основными средствами обеспечения безопасности данных. Навыками работы с нормативными документами по администрированию баз данных. Средствами обеспечения безопасности данных. Навыками разработки и администрирования базы данных. Навыками организации безопасности систем баз данных. Средствами обеспечения безопасности данных и АИС.
ОПК-3 способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности	

Знать	Виды аутентификации и принципы, на которых они основаны. Принципы программирования различных видов карт и ключей доступа. Типы атак на системы данных, использующих различные виды аутентификации
Уметь	Настраивать систему организации и контроля доступа различного вида. Анализировать и находить решения по защите от атак на системы данных, использующих различные виды аутентификации. Устанавливать средства защиты БД.
Владеть	Навыками настройки и администрирования средств защиты БД. Навыками разработки системы защиты с учетом особенностей защиты информации, обрабатываемой в СУБД. Навыками анализа критериев оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем.

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 6 зачетных единиц 216 акад. часов, в том числе:

– контактная работа – 127 акад. часов:

– аудиторная – 122 акад. часов;

– внеаудиторная – 5 акад. часов

– самостоятельная работа – 53,3 акад. часов;

– подготовка к экзамену – 35,7 акад. часа

Форма аттестации - зачет, экзамен

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа студента	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код компетенции
		Лек.	лаб. зан.	практ. зан.				
1. Общие положения обеспечения безопасности доступа к данным.								
1.1 Предмет и содержание дисциплины. Обеспечение безопасности доступа к данным.	5	3		4/2И	1	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Подготовка к АКР.	Аудиторная контрольная работа	ОПК-3
1.2 Задачи защиты информации обеспечения безопасности доступа к данным.		2		4/2И	1	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Подготовка к АКР.	Аудиторная контрольная работа	ПК-23, ОПК-3
Итого по разделу		5		8/4И	2			
2. Обеспечение надежной аутентификации.								

2.1 Факторы аутентификации.	5	3		4/2И	1	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Подготовка к АКР и КТ.	Тестирование, аудиторная контрольная работа	ПК-23, ОПК-3
2.2 Аутентификация с использованием OTP-токенов. Аутентификация с помощью биометрических характеристик. Анализ недостатков методов.		2		4/2И	1	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Подготовка к АКР и КТ.	Аудиторная контрольная работа	
Итого по разделу		5		8/4И	2			
3. Управление доступом к данным.								
3.1 СКУД на базе контактных смарт-карт. СКУД на базе бесконтактных RFID смарт-карт. СКУД на базе биометрических систем.	5	2		5/2И	1	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Подготовка к АКР.	Аудиторная контрольная работа	ПК-23, ПК-25, ОПК-3
3.2 СКУД на базе ключей eToken. СКУД на базе ключей iButton.		2		5/2И	2	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Подготовка к АКР.	Аудиторная контрольная работа	ПК-23, ПК-25, ОПК-3
Итого по разделу		4		10/4И	3			
4. Парольные политики.								
4.1 Методы парольной аутентификации.	5	2		5/2И	2	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Подготовка к КТ.	Компьютерное тестирование	ПК-23, ПК-25, ОПК-3

4.2 Аутентификация с помощью запоминаемого пароля. Недостатки методов аутентификации с помощью запоминаемого пароля.		2		5	2	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Подготовка к КТ.	Компьютерное тестирование	ПК-23, ПК-25, ОПК-3
Итого по разделу		4		10/2И	4			
5. Зачет								
5.1 Зачет	5				6	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Подготовка к зачету.	Зачет	ПК-23, ПК-25, ОПК-3
Итого по разделу					6			
Итого за семестр		18		36/14И	17		зачёт	
6. Документирование баз данных с учетом требований по обеспечению информационной								
6.1 Классы безопасности. Требования, предъявляемые к различным классам безопасности.	6	4		2/2И	6	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Подготовка к КТ.	Компьютерное тестирование	ПК-23, ПК-25, ОПК-3
6.2 Требования к документации с учетом класса безопасности.		4		4/2И	4	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Подготовка к КТ.	Компьтерное тестирование	ПК-23, ПК-25, ОПК-3
Итого по разделу		8		6/4И	10			
7. Атаки на системы данных.								

7.1 Атаки на системы данных, в которых используется аутентификация на основе пароля, и способы защиты от них.	6	2		2	4	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Подготовка к АКР.	Аудиторная контрольная работа	ПК-23, ПК-25, ОПК-3
7.2 Атаки на системы данных, использующие аутентификацию с помощью биометрических характеристик, и способы защиты от них.		4		4/2И	4	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Подготовка к АКР.	Аудиторная контрольная работа	ПК-23, ПК-25, ОПК-3
7.3 SQL-инъекции		4		2	2	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Подготовка к АКР.	Аудиторная контрольная работа	ПК-23, ПК-25, ОПК-3
Итого по разделу		10		8/2И	10			
8. Применение средств криптографической защиты информации (СКЗИ).								
8.1 Применение средств криптографической защиты информации (СКЗИ), хранящейся в базах данных, от НСД.	6	4		5/3И	4	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Подготовка к АКР.	Аудиторная контрольная работа	ПК-23, ПК-25, ОПК-3
8.2 Способы и средства криптографической защиты баз данных.		4		5/3И	4	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Подготовка к АКР.	Аудиторная контрольная работа	ПК-23, ПК-25, ОПК-3
Итого по разделу		8		10/6И	8			

9. СКЗИ «Крипто БД».								
9.1 Состав и совместимость СКЗИ «Крипто БД». Реализуемые алгоритмы криптографического преобразования в СКЗИ «Крипто БД».	6	2		3	2,3	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Подготовка к АКР.	Аудиторная контрольная работа	
9.2 Использование «Крипто БД» в облачных средах. Основные принципы работы «Крипто БД».		2		3/2И	2	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Подготовка к АКР.	Аудиторная контрольная работа	ПК-23, ПК-25, ОПК-3
9.3 Анализ угроз и уязвимостей СУБД Oracle		4		4	4	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Подготовка к КТ.	Компьютерное тестирование	ПК-23, ПК-25, ОПК-3
Итого по разделу		8		10/2И	8,3			
10. Экзамен								
10.1 Экзамен	6					Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Подготовка к экзамену.	Экзамен	ПК-23, ПК-25, ОПК-3
Итого по разделу								
Итого за семестр		34		34/14И	36,3		экзамен	
Итого по дисциплине		52		70/28И	53,3		зачет, экзамен	ОПК-3,ПК-23,ПК-25

5 Образовательные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины используются:

1) Традиционная технология, включающая в себя объяснение преподавателя на лекциях, самостоятельную работу с учебной и справочной литературой по дисциплине, выполнение заданий по методическим указаниям. Формы учебных занятий с использованием традиционных технологий:

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины используются:

1) Традиционная технология, включающая в себя объяснение преподавателя на лекциях, самостоятельную работу с учебной и справочной литературой по дисциплине, выполнение заданий по методическим указаниям. Формы учебных занятий с использованием традиционных технологий:

a) Вводная лекция – для целостного представления об учебном предмете и анализа учебно-методической литературы;

b) Обзорные лекции – для систематизации научных знаний на высоком уровне с использованием ассоциативных связей в процессе представления и осмысления информации;

c) Информационная лекция – последовательное изложение материала в дисциплинарной логике, осуществляемое преимущественно вербальными средствами (монолог преподавателя);

d) Семинар – беседа преподавателя и обучающихся, обсуждение заранее подготовленных сообщений по каждому вопросу плана занятия с единым для всех перечнем рекомендуемой обязательной и дополнительной литературы;

e) Практическое занятие, посвященное освоению конкретных умений и навыков по предложенному алгоритму;

f) Лабораторная работа – организация учебной работы с реальными материальными и информационными объектами, экспериментальная работа с аналоговыми моделями реальных объектов.

2) Разделно-компетентностная технология, включающая в себя жесткое структурирование содержания учебного материала, сопровождающаяся обязательными блоками домашних заданий, контрольных работ и тестированием по каждой теме содержания курса. Формы учебных занятий с использованием Разделно-компетентностной технологии:

a) Кейс-методы – для овладения системой знаний и умений и творческого их использования в профессиональной деятельности и самообразовании; для квалифицированного и независимого решения профессиональных задач; для ориентации в многообразии учебных программ, пособий, литературы и выбора наиболее эффективных в применении к конкретной ситуации; для осуществления саморефлексии для дальнейшего профессионального, творческого роста и социализации личности.

3) Интерактивные технологии – организация образовательного процесса, которая предполагает активное и нелинейное взаимодействие всех участников, достижение на этой основе личностно значимого для них образовательного результата. Наряду со специализированными технологиями такого рода принцип интерактивности прослеживается в большинстве современных образовательных технологий. Интерактивность подразумевает субъект-субъектные отношения в ходе образовательного процесса и, как следствие, формирование саморазвивающейся информационно-ресурсной среды. Формы учебных занятий с использованием интерактивных технологий:

a) Case-study – для анализа реальных проблемных ситуаций и поиска лучших вариантов решений, разбор результатов тематических контрольных работ,

анализ ошибок, совместный поиск вариантов рационального решения проблемы.

b) Методы IT – для применения компьютеров в процессе освоения дисциплины и доступа к ЭОР кафедры и Интернет-ресурсам.

c) Лекция «обратной связи» – лекция–провокация (изложение материала с заранее запланированными ошибками), лекция-беседа, лекция-дискуссия, лекция-прессконференция.

d) Семинар-дискуссия – коллективное обсуждение какого-либо спорного вопроса, проблемы, выявление мнений в группе (межгрупповой диалог, дискуссия как спор-диалог).

e) Контекстное обучение – для мотивации обучающихся к усвоению знаний путем выявления связей между конкретным знанием и его применение. Овладев в рамках изучения дисциплины навыками обеспечения безопасности информации с помощью типовых программных средств, обучающийся приобретет способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности;

f) Междисциплинарное обучение – для использования знаний из различных областей, их группировки и концентрации в контексте решаемой задачи. Для реализации данного метола обучения обучающимся выдаются задания по решения задач из другой предметной области.

4) Технологии проблемного обучения – организация образовательного процесса, которая предполагает постановку проблемных вопросов, создание учебных проблемных ситуаций для стимулирования активной познавательной деятельности обучающихся. Формы учебных занятий с использованием технологий проблемного обучения:

a) Проблемная лекция – изложение материала, предполагающее постановку проблемных и дискуссионных вопросов, освещение различных научных подходов, авторские комментарии, связанные с различными моделями интерпретации изучаемого материала.

b) Лекция «вдвоем» (бинарная лекция) – изложение материала в форме диалогического общения двух преподавателей (например, реконструкция диалога представителей различных научных школ, «ученого» и «практика» и т.п.).

c) Практическое занятие в форме практикума – организация учебной работы, направленная на решение комплексной учебно-познавательной задачи, требующей от обучающегося применения как научно-теоретических знаний, так и практических навыков.

d) Практическое занятие на основе кейс-метода – обучение в контексте моделируемой ситуации, воспроизводящей реальные условия научной, производственной, общественной деятельности. Обучающиеся должны проанализировать ситуацию, разобраться в сути проблем, предложить возможные решения и выбрать лучшее из них. Кейсы базируются на реальном фактическом материале или же приближены к реальной ситуации. разбор результатов тематических контрольных работ, анализ ошибок, совместный поиск вариантов рационального решения учебной проблемы.

5) Игровые технологии – организация образовательного процесса, основанная на реконструкции моделей поведения Формы учебных занятий с использованием предложенных сценарных условий. Формы учебных занятий с использованием игровых технологий:

a) Учебная игра – форма воссоздания предметного и социального содержания будущей профессиональной деятельности специалиста, моделирования таких систем отношений, которые характерны для этой деятельности как целого.

b) Деловая игра – моделирование различных ситуаций, связанных с выработкой и принятием совместных решений, обсуждением вопросов в режиме «мозгового штурма», реконструкцией функционального взаимодействия в коллективе и

т.п.

c) Ролевая игра – имитация или реконструкция моделей ролевого поведения в предложенных сценарных условиях.

6) Технологии проектного обучения – организация образовательного процесса в соответствии с алгоритмом поэтапного решения проблемной задачи или выполнения учебного задания. Проект предполагает совместную учебно-познавательную деятельность группы обучающихся, направленную на выработку концепции, установление целей и задач, формулировку ожидаемых результатов, определение принципов и методик решения поставленных задач, планирование хода работы, поиск доступных и оптимальных ресурсов, поэтапную реализацию плана работы, презентацию результатов работы, их осмысление и рефлексию. Основные типы проектов:

a) Исследовательский проект – структура приближена к формату научного исследования (доказательство актуальности темы, определение научной проблемы, предмета и объекта исследования, целей и задач, методов, источников, выдвижение гипотезы, обобщение результатов, выводы, обозначение новых проблем).

b) Творческий проект, как правило, не имеет детально проработанной структуры; учебно-познавательная деятельность обучающихся осуществляется в рамках рамочного задания, подчиняясь логике и интересам участников проекта, жанру конечного результата (газета, фильм, праздник, издание, экскурсия и т.п.).

c) Информационный проект – учебно-познавательная деятельность с ярко выраженной эвристической направленностью (поиск, отбор и систематизация информации о каком-то объекте, ознакомление участников проекта с этой информацией, ее анализ и обобщение для презентации более широкой аудитории).

7) Информационно-коммуникационные образовательные технологии – организация образовательного процесса, основанная на применении специализированных программных сред и технических средств работы с информацией. Формы учебных занятий с использованием информационно-коммуникационных технологий:

a) Лекция-визуализация – изложение содержания сопровождается презентацией (демонстрацией учебных материалов, представленных в различных знаковых системах, в т.ч. иллюстративных, графических, аудио- и видеоматериалов).

b) Практическое занятие в форме презентации – представление результатов проектной или исследовательской деятельности с использованием специализированных программных сред.

6. Учебно-методическое обеспечение самостоятельной работы обучающихся

Аудиторная самостоятельная работа обучающихся на практических занятиях осуществляется под контролем преподавателя в виде решения задач и выполнения упражнений, которые определяет преподаватель для обучающихся с использованием **методов IT .**

Внеаудиторная самостоятельная работа обучающихся осуществляется в виде чтения литературы по соответствующему разделу с проработкой материала и выполнения домашних заданий с консультациями преподавателя, а так же с применением **Кейс-технологий.**

Задания и вопросы по разделам

Раздел 1-4

Вопросы:

1. Процедуры, выполняемые при регистрации пользователя в системе.
2. Перечислить элементы аутентификации.
3. Привести примеры факторов аутентификации.
4. Для чего служит механизм управления доступом?
5. Структура команд APDU. Примеры команд APDU.
6. Для чего необходимы парольные политики?
7. Методы парольной аутентификации.
8. Описать принципы работы биометрических систем.
9. Описать принцип работы OTP-токена.
10. Способы аутентификации пользователя при использовании OTP-токена.

Задания:

1. Построить СКУД на базе контактных смарт-карт.
2. Построить СКУД на базе бесконтактных RFID смарт-карт.
3. Построить СКУД на базе биометрических систем.
4. Построить СКУД на базе ключей eToken.
5. Построить СКУД на базе ключей iButton.

Раздел 5-8

Вопросы:

1. Привести примеры атак на системы данных, в которых используется аутентификация на основе пароля, и способы защиты от них.
2. Привести примеры атак на системы данных, использующие аутентификацию с помощью биометрических характеристик, и способы защиты от них.
3. Привести примеры атак на системы данных, использующие аутентификацию с помощью OTP-токенов, и способы защиты от них.
4. Применение криптографии с открытым ключом для шифрования сообщения.
5. ЭЦП. Примеры использования.
6. Реализуемые алгоритмы криптографического преобразования в СКЗИ «Крипто БД».

Задания:

1. Для сервера базы данных и для каждого пользователя, включая администраторов безопасности, создать по одной ключевой паре (открытый и закрытый ключи) с использованием СКЗИ «Крипто БД».

7. Оценочные средства для проведения промежуточной аттестации

а) Планируемые результаты обучения и оценочные средства для проведения промежуточной аттестации:

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
ОПК-3 - способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности**.**		
Знать	*Виды аутентификации и принципы, на которых они основаны.* *Принципы программирования различных видов карт и ключей доступа.* *Типы атак на системы данных, использующих различные виды аутентификации*	Вопросы для зачета: 1. Процедуры, выполняемые при регистрации пользователя в системе. 2. Перечислить элементы аутентификации. 3. Привести примеры факторов аутентификации. 4. Для чего служит механизм управления доступом? 5. Структура команд APDU. Примеры команд APDU. 6. Для чего необходимы парольные политики? 7. Методы парольной аутентификации. 8. Описать принципы работы биометрических систем. 9. Описать принцип работы OTP-токена. 10. Способы аутентификации пользователя при использовании OTP-токена.
Уметь	*Настраивать систему организации и контроля доступа различного вида.* *Анализировать и находить решения по защите от атак на системы данных, использующих различные виды аутентификации.* *Устанавливать средства защиты БД.*	1. Провести анализ атак на системы данных, в которых используется аутентификация на основе пароля, и найти способы защиты от них. 2. Провести анализ атак на системы данных, использующие аутентификацию с помощью биометрических характеристик, и найти способы защиты от них. 3. Провести анализ атак на системы данных, использующие аутентификацию с помощью OTP-токенов, и найти способы защиты от них.
Владеть	*Навыками настройки и администрирования средств защиты БД.* *Навыками разработки системы защиты с учетом особенностей защиты информации, обрабатываемой в СУБД.* *Навыками анализа критериев оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем.*	1. Запрограммировать смарт карту. 2. Внести в БД биометрической системы аутентификации 2х администраторов. В качестве идентификаторов использовать отпечаток пальца и модель лица. 3. Внести в БД биометрической системы аутентификации 2х пользователей. В качестве идентификаторов использовать отпечаток пальца или пароль. 4. Запрограммировать 2 ключа iButton на блокировку входа. 5. Запрограммировать 2 ключа iButton на администрирование системы.
ПК-23 - способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа		
Знать	*Методы формирования требований по защите информации, обрабатываемой в*	Вопросы к экзамену: 1. Процедуры, выполняемые при регистрации пользователя в системе.

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	СУБД. *Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации, обрабатываемой в СУБД.* *Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем.* *Организационные меры по защите информации, обрабатываемой в СУБД.*	2. Перечислить элементы аутентификации. 3. Привести примеры факторов аутентификации. 4. Для чего служит механизм управления доступом? 5. Структура команд APDU. Примеры команд APDU. 6. Для чего необходимы парольные политики? 7. Методы парольной аутентификации. 8. Привести примеры атак на системы данных, в которых используется аутентификация на основе пароля, и способы защиты от них. 9. Привести примеры атак на системы данных, использующие аутентификацию с помощью биометрических характеристик, и способы защиты от них.
Уметь	*Использовать методы формирования требований по защите информации, обрабатываемой в СУБД.* *Классифицировать средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации, обрабатываемой в СУБД.* *Организовывать безопасность АРМ, на которых установлена СУБД.*	1. Построить СКУД на базе контактных смарт-карт. 2. Построить СКУД на базе бесконтактных RFID смарт-карт. 3. Построить СКУД на базе биометрических систем. 4. Построить СКУД на базе ключей eToken. 5. Построить СКУД на базе ключей iButton. 6. Настроить систему видеонаблюдения помещения, в котором находиться ОИ.
Владеть	*Методами формирования требований по защите информации, обрабатываемой в СУБД.* *Навыками анализа методов формирования требований по защите информации, обрабатываемой в СУБД.*	1. Обеспечить конфиденциальности и контроль целостности информации в БД с использованием СКЗИ «Крипто БД» по требованиям ИБ. 2. Провести мониторинг и аудит доступа к зашифрованным данным БД.
ПК-25 - способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций		
Знать	*Принципы работы баз данных.* *Основные средства обеспечения безопасности данных.* *Принципы администрирования баз данных. Средства обеспечения безопасности данных.* *Организацию защиты информации баз данных.* *Сравнительный анализ эффективности применения*	Вопросы к экзамену: 10. Описать принципы работы биометрических систем. 11. Описать принцип работы OTP-токена. 12. Способы аутентификации пользователя при использовании OTP-токена. 13. Привести примеры атак на системы данных, использующие аутентификацию с помощью OTP-токенов, и способы защиты от них. 14. Применение криптографии с открытым

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	средств обеспечения безопасности данных.	ключом для шифрования сообщения. 15. ЭЦП. Примеры использования. 16. Реализуемые алгоритмы криптографического преобразования в СКЗИ «Крипто БД». 17. Архитектура СКЗИ «Крипто БД». 18. Этапы эксплуатации СКЗИ «Крипто БД» и задачи, выполняемые на каждом этапе.
Уметь	*Анализировать работоспособность базы данных.* *Принимать участие в настройке средств обеспечения безопасности данных, обрабатываемых в СУБД.* *Самостоятельно применять средства обеспечения безопасности данных.* *Участвовать в восстановлении работоспособности систем баз данных при возникновении нештатных ситуаций.* *Организовывать безопасность систем баз данных.*	1. Провести анализ инцидентов безопасности с использованием СКЗИ «Крипто БД». 2. Настроить СКЗИ «Крипто БД».
Владеть	*Основными средствами обеспечения безопасности данных.* *Навыками работы с нормативными документами по администрированию баз данных.* *Средствами обеспечения безопасности данных.* *Навыками разработки и администрирования базы данных.* *Навыками организации безопасности систем баз данных.* *Средствами обеспечения безопасности данных и АИС.*	1. Для сервера базы данных и для каждого пользователя, включая администраторов безопасности, создать по одной ключевой паре (открытый и закрытый ключи) с использованием СКЗИ «Крипто БД». 2. Настроить доступ Администраторов СУБД к хранящейся в базе информации согласно матрице доступа с использованием СКЗИ «Крипто БД».

б) Порядок проведения промежуточной аттестации, показатели и критерии оценивания:

Показатели и критерии оценивания зачета:

– на **«зачтено»** – обучающийся должен показать пороговый уровень знаний на уровне воспроизведения и объяснения информации;

– на **«не зачтено»** – обучающийся не может показать знания на уровне воспроизведения и объяснения информации.

Показатели и критерии оценивания экзамена:

– на оценку **«отлично»** – обучающийся должен показать высокий уровень знаний не только на уровне воспроизведения и объяснения информации, но и интеллектуальные

навыки решения проблем и задач, нахождения уникальных ответов к проблемам, оценки и вынесения критических суждений;

– на оценку **«хорошо»** – обучающийся должен показать средний уровень знаний не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач;

– на оценку **«удовлетворительно»** – обучающийся должен показать пороговый уровень знаний на уровне воспроизведения и объяснения информации, навыки решения типовых задач;

– на оценку **«неудовлетворительно»** – обучающийся не может показать знания на уровне воспроизведения и объяснения информации, не может показать навыки решения типовых задач.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1. Полищук, Ю. В. Базы данных и их безопасность : учебное пособие / Ю.В. Полищук, А.С. Боровский. — Москва : ИНФРА-М, 2020. — 210 с. — (Высшее образование: Специалитет). — DOI 10.12737/1011088. - ISBN 978-5-16-107421-3. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1011088 (дата обращения: 26.02.2020)

2. Маркин, А. В. Программирование на SQL в 2 ч. Часть 1 : учебник и практикум для вузов / А. В. Маркин. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 403 с. — (Высшее образование). — ISBN 978-5-534-12256-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/452357 (дата обращения: 24.02.2020).

3. Маркин, А. В. Программирование на SQL в 2 ч. Часть 2 : учебник и практикум для вузов / А. В. Маркин. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 340 с. — (Высшее образование). — ISBN 978-5-534-12258-9. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/451185 (дата обращения: 24.02.2020).

б) Дополнительная литература:

1. Зашита информации : учеб. пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - Москва : РИОР: ИНФРА-М, 2019. - 400 с. - (Высшее образование). - DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-16-106478-8. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1018901 (дата обращения: 26.02.2020)

2. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/422772(дата обращения: 24.02.2020).

3. Внуков, А. А. Защита информации в банковских системах : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2018. — 246 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-01679-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/414083 (дата обращения: 24.02.2020).

4. Сетевая защита информации. Лабораторный практикум: учебное пособие [для вузов] / Д. Н. Мазнин [и др.]; Магнитогорский гос. технический ун-т им. Г. И. Носова. - Магнитогорск : МГТУ им. Г. И. Носова, 2019. - 1 CD-ROM. - Загл. с титул. экрана. - URL: https://magtu.informsystema.ru/uploader/fileUpload?name=3824.pdf&show=dcatalogues/1/1530260/3824.pdf&view=true (дата обращения: 22.10.2019). – Макрообъект*. - ISBN 978-5-9967-1605-0. - Текст: электронный. - Сведения доступны также на CD-ROM.

*РЕЖИМ ПРОСМОТРА МАКРООБЪЕКТОВ

1. Перейти по адресу электронного каталога https://magtu.informsystema.ru .
2. Произвести авторизацию (Логин: Читатель1 Пароль: 111111)
3. Активизировать гиперссылку макрообъекта*.

*При открытии макрообъектов учитывайте настройки антивирусной защиты

в) Методические указания:

1. Методические указания по выполнению практических работ (Приложение 1)

2. Методические указания по выполнению внеаудиторных самостоятельных работ (Приложение 2)

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия лицензии
MS Windows 7 Professional(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office 2007 Professional	№ 135 от 17.09.2007	бессрочно
7Zip	свободно распространяемое ПО	бессрочно
MS SQL Server Management Studio	свободно распространяемое ПО	бессрочно
Oracle My SQL Workbench Community Edition	свободно распространяемое ПО	бессрочно
Oracle SQL Developer	свободно распространяемое ПО	бессрочно
Oracle SQL Developer Data Modeler	свободно распространяемое ПО	бессрочно

MS Windows 10 Professional (для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Windows Server(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
eTokenSecurLogon for Oracle	К-271-12 от 16.10.2012	бессрочно
СКЗИ КриптоПро CSP	К-271-12 от 16.10.2012	бессрочно
Браузер Mozilla Firefox	свободно распространяемое ПО	бессрочно
Браузер Yandex	свободно распространяемое ПО	бессрочно
MS Windows XP Professional(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
LibreOffice	свободно распространяемое ПО	бессрочно
FAR Manager	свободно распространяемое ПО	бессрочно
Linux Calculate	свободно распространяемое ПО	бессрочно

Профессиональные базы данных и информационные справочные системы

Название ресурса	Ссылка
Информационная система - Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации ФСТЭК России	URL: https://fstec.ru/normotvorcheskaya/tekhnicheskaya-zashchita-informatsii
Информационная система - Банк данных угроз безопасности информации ФСТЭК России	URL: https://bdu.fstec.ru/
Национальная информационно-аналитическая система – Российский индекс научного цитирования (РИНЦ)	URL: https://elibrary.ru/project_risc.asp

Поисковая система Академия Google (Google Scholar)	URL: https://scholar.google.ru/
Информационная система - Единое окно доступа к информационным ресурсам	URL: http://window.edu.ru/
Федеральное государственное бюджетное учреждение «Федеральный институт промышленной собственности»	URL: http://www1.fips.ru/

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

Лаборатория программно-аппаратных средств обеспечения информационной безопасности:

1. СКЗИ Крипто БД(лицензия: договор К-271-12 от 16.10.12, бессрочно)
2. Электронный ключ Guardant
3. Электронный ключ Etoken
4. Устройство идентификации (Электронный ключ Guardant ID сертифицированный)
5. Компьютер Destene Volution i560 на базе Windows Server 2008 R2(Standart) MSDN
6. ПЭВМ на базе Windows 7 – 12 шт

Лаборатория защищенных автоматизированных систем:

1. Комплект учебного оборудования "Системы контроля доступа"
2. Комплект учебного оборудования "Системы мониторинга информационной безопасности"

Лекционные аудитории (ауд. 2124, ауд. 226, ауд. 365, ауд. 388 и т.д.):

Мультимедийные средства хранения, передачи и представления информации

Компьютерные классы (ауд. 372, ауд. 245, ауд. 247, ауд. 144, ауд. 142 и т.д.):

Персональные компьютеры с ПО и выходом в Интернет и доступом в электронную информационно-образовательную среду университета.

ПРИЛОЖЕНИЕ 1

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
ПО ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ РАБОТ

Рекомендации направлены на оказание методической помощи обучающимся при выполнении практических занятий.

Практическое занятие – это занятие, проводимое под руководством преподавателя в учебной аудитории (компьютерном классе университета или учебной специализированной лаборатории университета), направленное на углубление научно-теоретических знаний и получение практических навыков решения типовых и прикладных задач.

Целью практических занятий является формирование и отработка практических умений и навыков, необходимых в последующей деятельности обучающихся.

Основными задачами практических занятий являются:

- углубление уровня освоения общекультурных и профессиональных компетенций;
- обобщение, систематизация, углубление, закрепление полученных практических знаний по конкретным темам дисциплин различных циклов;
- приобретение обучающимися умений и навыков использования современных теоретических знаний в решении конкретных практических задач;
- развитие профессионального мышления, профессиональной и познавательной мотивации.

Перечень тем практических занятий определяется рабочей программой дисциплины. План практических занятий отвечает общей направленности лекционного курса и соотнесен с ним в последовательности тем.

Структура практического занятия включает следующие компоненты: вступительная часть; ответы на вопросы обучающихся; практическая часть; заключительное слово преподавателя. Во вступительной части объявляется тема текущего практического занятия, ставится его цели и задачи, проверяется исходный уровень готовности обучающихся к практическому занятию (выполнение тестов, контрольные вопросы и т.п.)

На практическом занятии преподаватель может использовать разнообразные образовательные технологии (методы IT, работа в команде, case-study, проблемное обучение, учебные дискуссии и т.п.) по своему выбору для достижения качественного уровня обучения.

Правила по технике безопасности для обучающихся при проведении практических работ

Общие правила:

1. Практические работы проводятся под наблюдением преподавателя. К выполнению практических работ обучающиеся допускаются только после прослушивания инструктажа по технике безопасности, правилам поведения, противопожарным мерам в компьютерном классе и специализированных лабораториях.
2. Обучаемый должен строго выполнять правила техники безопасности и санитарно-гигиенические нормы при работе в компьютерных классах и специализированных лабораториях университета.

Порядок выполнения практических работ

При подготовке к выполнению практических работ обучающийся должен повторить теоретический материал, необходимый для выполнения заданий по текущей теме.

Практическая работа выполняется каждым обучающимся самостоятельно, согласно индивидуальному заданию.

Обучающиеся, пропустившие занятия, выполняют практические работы во внеурочное время.

После выполнения каждой практической работы обучающийся демонстрирует результат выполнения преподавателю, отвечает на вопросы. Преподаватель оценивает работу в соответствии с заданными критериями оценки практических работ.

Правила оформления результатов и оценивания практической работы

Результаты выполненной практической работы оформляются в соответствии с требованиями к выполнению конкретной работы.

Практическая работа считается выполненной, если обучающийся набрал балл, который составляет половину максимального количества баллов.

Для оценивания работы прилагается следующие критерии.

Оценка «отлично» – работа выполнена в полном объеме и без замечаний.

Оценка «хорошо» – работа выполнена правильно с учетом 2-3 несущественных ошибок, исправленных самостоятельно по требованию преподавателя.

Оценка «удовлетворительно» – работа выполнена правильно не менее чем на половину или допущена существенная ошибка.

Оценка «неудовлетворительно» – допущены две (и более) существенные ошибки в ходе работы, которые обучающийся не может исправить даже по требованию преподавателя, или работа не выполнена.

ПРИЛОЖЕНИЕ 2

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ВНЕАУДИТОРНЫХ САМОСТОЯТЕЛЬНЫХ РАБОТ

Общие положения

Настоящие методические указания предназначены для организации внеаудиторной самостоятельной работы обучающихся и оказания помощи в самостоятельном изучении теоретического и реализации компетенций обучаемых.

Данные методические указания не являются учебным пособием, поэтому перед началом выполнения самостоятельного задания следует изучить соответствующие разделы лекционных занятий, материалов образовательного портала, разделов основной и дополнительной литературы, представленных в пункте 8. «Учебно-методическое и информационное обеспечение дисциплины (модуля)» данной РПД.

Цели и задачи самостоятельной работы

Цель самостоятельной работы – содействие оптимальному усвоению учебного материала обучающимися, развитие их познавательной активности, готовности и потребности в самообразовании.

Задачи самостоятельной работы:

- повышение исходного уровня владения информационными технологиями;
- углубление и систематизация знаний;
- постановка и решение стандартных задач профессиональной деятельности;
- развитие работы с различной по объему и виду информацией, учебной и научной литературой;
- практическое применение знаний, умений;
- самостоятельно использование стандартных программных средств сбора, обработки, хранения и защиты информации
- развитие навыков организации самостоятельного учебного труда и контроля за его эффективностью.

Виды внеаудиторной самостоятельной работы и формы контроля и время на выполнение каждого вида самостоятельной работы указаны в пункте 4. «Структура и содержание дисциплины» данной РПД.

Порядок выполнения

При выполнении текущей внеаудиторной самостоятельной работы обучающемуся следует придерживаться следующего порядка действий:

1) внимательно изучить соответствующие теоретические разделы дисциплины, пользуясь материалами (лекционными, презентационными, аудио-визуальными):
   a) предоставляемыми преподавателем на лекционных занятиях;
   b) предоставляемыми преподавателем в рамках электронных образовательных курсов;
   c) содержащимися в учебниках и учебных пособиях ЭБС (электронно-библиотечных систем), электронных каталогов университета и интернет-ресурсов.
2) Подробно разобрать типовые примеры решения задач, рассмотренные в рамках аудиторной контактной работы с преподавателем.
3) Применить полученные теоретические знания и практические навыки к решению индивидуальных заданий, к прохождению компьютерных тестирований.
4) При необходимости, сформировать перечень вопросов, вызвавших затруднения в процессе самостоятельной работы. Обсудить возникшие вопросы с обучающимися группы, в рамках командно-проектной работы, и с преподавателем, в рамках консультационной помощи, реализованной либо в контактной форме, либо средствами информационно-образовательной среды ВУЗа.

Критерии оценки внеаудиторных самостоятельных работ

Качество выполнения внеаудиторной самостоятельной работы обучающихся оценивается посредством текущего контроля самостоятельной работы обучающихся с использованием балльно-рейтинговой системы.

В качестве форм текущего контроля по дисциплине используются: индивидуальные задания, аудиторные контрольные работы, компьютерное тестирование.

Максимальное количество баллов обучающийся получает, если:

- выполняет индивидуальные задания в соответствии со всеми заявленными требованиями;
- дает правильные формулировки, точные определения, понятия терминов;
- может обосновать рациональность решения текущей задачи.;
- обстоятельно с достаточной полнотой излагает соответствующую теоретический раздел;
- правильно отвечает на дополнительные вопросы преподавателя, имеющие целью выяснить степень понимания им данного материала.

50~85% от максимального количества баллов обучающийся получает, если:

- неполно (не менее 70% от полного), но правильно выполнено задание;

- при изложении были допущены 1-2 несущественные ошибки, которые он исправляет после замечания преподавателя;
- дает правильные формулировки, точные определения, понятия терминов;
- может обосновать свой ответ, привести необходимые примеры;
- правильно отвечает на дополнительные вопросы преподавателя, имеющие целью выяснить степень понимания им данного материала.

36~50% от максимального количества баллов обучающийся получает, если:

- неполно (не менее 50% от полного), но правильно изложено задание;
- при изложении была допущена 1 существенная ошибка;
- знает и понимает основные положения данной темы, но допускает неточности в формулировке понятий;
- излагает выполнение задания недостаточно логично и последовательно;
- затрудняется при ответах на вопросы преподавателя.

35% и менее от максимального количества баллов обучающийся получает, если:

- неполно (менее 50% от полного) изложено задание;
- при изложении были допущены существенные ошибки. В "0" баллов преподаватель вправе оценить выполненное обучающимся задание, если оно не удовлетворяет требованиям, установленным преподавателем к данному виду работы или не было представлено для проверки.

Сумма полученных баллов по всем видам заданий внеаудиторной самостоятельной работы составляет рейтинговый показатель обучающегося. Рейтинговый показатель обучающегося влияет на выставление итоговой оценки по результатам изучения дисциплины.

Показатели и критерии оценивания полученных знаний представлены в пункте 7.б) «Оценочные средства для проведения промежуточной аттестации» данной РПД.