МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

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

УТВЕРЖДАЮ:
Директор института
Энергетики и автоматизированных систем
_____ С.И. Лукьянов
«26» сентября 2018 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

БЕЗОПАСНОСТЬ СИСТЕМ БАЗ ДАННЫХ
наименование дисциплины

Специальность
10.05.03 Информационная безопасность автоматизированных систем
шифр наименование специальности

Специализация программы
Обеспечение информационной безопасности распределенных информационных систем
наименование специализации

Уровень высшего образования
специалитет

Форма обучения
очная

Институт	Энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	3
Семестр	5,6

Магнитогорск
2018 г.

Рабочая программа составлена на основе ФГОС ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем», утвержденного приказом МОиН РФ от 01.12.2016 № 1509.

Рабочая программа рассмотрена и одобрена на заседании кафедры
Информатики и информационной безопасности
(наименование кафедры - разработчика)

«07» сентября 2018 г., протокол № 1.

Зав. кафедрой _____ / И.И. Баранкова/
(подпись) (И.О. Фамилия)

Рабочая программа одобрена методической комиссией
института Энергетики и автоматизированных систем
(наименование факультета (института) - исполнителя)

«26» сентября 2018 г., протокол № 1.

Председатель _____ / С.И. Лукьянов/
(подпись) (И.О. Фамилия)

Рабочая программа составлена: доцент кафедры ИиИБ, к.т.н.
(должность, ученая степень, ученое звание)

_____ / У.В. Михайлова /
(подпись) (И.О. Фамилия)

Рецензент: зав. кафедрой Бизнес-информатики
и информационных технологий, к.п.н. профессор
(должность, ученая степень, ученое звание)

_____ / Г.Н. Чусавитина/
(подпись) (И.О. Фамилия)

Лист регистрации изменений и дополнений

№ п/п	Раздел программы	Краткое содержание изменения/дополнения	Дата, № протокола заседания кафедры	Подпись зав. кафедрой
1.	7	Переработка фонда оценочных средств	№ 1 от 07.09.2019	
2.	8	Обновление списка основной и дополнительной литературы	№ 1 от 07.09.2019	
3.	7	Переработка фонда оценочных средств	№ 1 от 04.09.2020	
4.	8	Обновление списка основной и дополнительной литературы	№ 1 от 04.09.2020	

1. Цели освоения дисциплины

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 в структуре ООП подготовки специалиста

Дисциплина «Безопасность систем баз данных» входит в цикл дисциплин (базовая часть) Б1.Б.25 образовательной программы по специальности 10.05.03 Информационная безопасность автоматизированных систем.

Успешное усвоение материала предполагает знание обучающимися основных положений курсов «Информатика», «Организация ЭВМ и вычислительных систем», «Введение в специальность», «Основы информационной безопасности», «Информационные технологии. Базы данных».

Дисциплина является предшествующей для изучения дисциплин: «Управление информационной безопасностью», «Разработка и эксплуатация защищенных автоматизированных систем», «Информационная безопасность распределенных информационных систем».

3. Компетенции обучающегося, формируемые в результате освоения дисциплины и планируемые результаты обучения

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

Структурный элемент компетенции	**Планируемые результаты обучения**
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.*
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,*

Структурный элемент компетенции	Планируемые результаты обучения
	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.*

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 6 зачетных единицы 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:

6 семестр – зачет, 7 семестр – экзамен.

Раздел дисциплины		Семестр	Аудиторная контактная работа (в акад. часах)			Вид самостоятельной работы	Формы текущего контроля и успеваемости и промежуточной	Код и структурный элемент
			Лекции	ятияПрактические	аСамостоятельная			нции
Раздел 1 **Общие положения обеспечения безопасности доступа к данным.**	**Тема 1.1.** Предмет и содержание дисциплины. Обеспечение безопасности доступа к данным.	**6**	**3**	**4/ 2И**	**1**	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Подготовка к АКР.	АКР-1	ПК-25-з, ПК-23-з
	Тема 1.2. Задачи защиты информации обеспечения безопасности доступа к данным.	**6**	**2**	**4/ 2И**	**1**			
Раздел 2 **Обеспечение надежной аутентификации.**	**Тема 2.1.** Факторы аутентификации.	**6**	**3**	**4/ 2И**	**1**	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Подготовка к АКР и КТ.	АКР-2 КТ-1	ПК-25-з, ПК-23-з, ОПК-3-зв
	Тема 2.2. Аутентификация с использованием OTP-токенов. Аутентификация с помощью биометрических характеристик. Анализ недостатков методов.	**6**	**2**	**4/ 2И**	**1**			
Раздел 3 **Управление доступом к данным.**	**Тема 3.1.** СКУД на базе контактных смарт-карт. СКУД на базе бесконтактных RFID смарт-карт. СКУД на базе биометрических систем.	**6**	**2**	**5/ 3И**	**1**	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Подготовка к АКР.	АКР-3 АКР-4	ПК-25-зув, ПК-23-зув, ОПК-3-зув
	Тема 3.2. СКУД на базе ключей eToken. СКУД на базе ключей iButton.	**6**	**2**	**5/ 3И**	**2**			
Раздел 4 **Парольные политики.**	**Тема 4.1.** Методы парольной аутентификации.	**6**	**2**	**5/ 3И**	**2**	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Подготовка к КТ.	КТ-2	ПК-25-зув, ПК-23-зув, ОПК-3-зув
	Тема 4.2 Аутентификация с помощью запоминаемого пароля. Недостатки методов аутентификации с помощью запоминаемого пароля.	**6**	**2**	**5/ 3И**	**2**			

	Зачет	**6**			**6**	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Подготовка к зачету.	Зачет	ПК-25-зув, ПК-23-зув, ОПК-3-зув
	Итого по семестру:	**6**	**18**	**36 / 20 И**	**17**			**72**
Раздел 5 **Документирование баз данных с учетом требований по обеспечению информационной безопасности.**	**Тема 5.1.** Классы безопасности. Требования, предъявляемые к различным классам безопасности.	**7**	**4**	**2/ 2И**	**3**	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Подготовка к КТ.	КТ-3	ПК-25-з, ПК-23-з, ОПК-3-з
	Тема 5.2. Требования к документации с учетом класса безопасности.	**7**	**4**	**4/ 2И**	**2**			
Раздел 6 **Атаки на системы данных.**	**Тема 6.1.** Атаки на системы данных, в которых используется аутентификация на основе пароля, и способы защиты от них.	**7**	**6**	**4/ 2И**	**3**	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Подготовка к АКР.	АКР-5	ПК-25-зув, ПК-23-зув, ОПК-3-зув
	Тема 6.2. Атаки на системы данных, использующие аутентификацию с помощью биометрических характеристик, и способы защиты от них.	**7**	**4**	**4/ 2И**	**2**			
Раздел 7. **Применение средств криптографической защиты информации (СКЗИ).**	**Тема 7.1.** Применение средств криптографической защиты информации (СКЗИ), хранящейся в базах данных, от НСД.	**7**	**4**	**5/ 3И**	**2**	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Подготовка к АКР.	АКР-6	ПК-25-зув, ПК-23-зув, ОПК-3-зув
	Тема 7.2. Способы и средства криптографической защиты баз данных.	**7**	**4**	**5/ 3И**	**2**			
Раздел 8 **СКЗИ «Крипто БД».**	**Тема 8.1.** Состав и совместимость СКЗИ «Крипто БД». Реализуемые алгоритмы криптографического преобразования в СКЗИ «Крипто БД».	**7**	**4**	**5/ 3И**	**2, 3**	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Подготовка к АКР.	АКР-7	ПК-25-зув, ПК-23-зув, ОПК-

	Тема 8.2. Использование «Крипто БД» в облачных средах. Основные принципы работы «Крипто БД».	**7**	**4**	**5/ 3И**	**2**			3-зув
	Экзамен	**7**			**35 ,7**	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Подготовка к экзамену.	Экзамен	ПК-25-зув, ПК-23-зув, ОПК-3-зув
	Итого по семестру		**34**	**34/ 20 И**	**36, 3+ 35, 7**			**144**
Итого по курсу			**54**	**72/ 40 И**	**53 ,3 +3 6**			**216**

Л – лекции, ПЗ – практические занятия, СР – самостоятельная работа, АКР – аудиторная контрольная работа, ИДЗ – индивидуальное задание, КТ – контрольное тестирование.

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:

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,*	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

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	использующих различные виды аутентификации	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 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.*	Вопросы к экзамену: 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. 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

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		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 средств обеспечения безопасности данных.*	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 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*	1. Провести анализ инцидентов безопасности с использованием СКЗИ «Крипто БД». 2. Настроить СКЗИ «Крипто БД».

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	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.*	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

а) Основная литература:

1. Базы данных. В 2-х кн. Кн. 2. Распределенные и удаленные базы данных [Электронный ресурс]: Учебник / В.П. Агальцов. - М.: ИД ФОРУМ: НИЦ Инфра-М, 2013. - 272 с.: ил.; - (Высшее образование). - Режим доступа: http://znanium.com/bookread.php?book=372740 - Загл. с экрана. - ISBN 978-5-8199-0394-0.

2. Информационная безопасность и защита информации: [Электронный ресурс]: учеб. пособие / Баранова Е.К., Бабаш А.В. - 3-е изд., перераб. и доп. - М. : РИОР: ИНФРА-М, 2017. - 322 с. - Режим доступа: http://znanium.com/bookread2.php?book=763644. - Загл. с экрана. – ISBN 978-5-369-01450-9.

3. Информационная безопасность и защита информации: [Электронный ресурс]: Учебное пособие / Баранова Е.К., Бабаш А.В., - 4-е изд., перераб. и доп. - М.:ИЦ РИОР, НИЦ ИНФРА-М, 2018. -

336 с. - Режим доступа:http://znanium.com/bookread2.php?book=957144. - Загл. с экрана. – ISBN 978-5-369-01761-6.

б) Дополнительная литература:

1. Баранкова И. И. Разработка БД в MS SQL Server с использованием SSMS [Электронный ресурс]: учебное пособие / И. И. Баранкова, У. В. Михайлова, Г. И. Лукьянов; МГТУ. - Магнитогорск: МГТУ, 2018. - 1 электрон. опт. диск (CD-ROM). - Режим доступа: https://magtu.informsystema.ru/uploader/fileUpload?name=3473.pdf&show=dcatalogues/1/1514290/3473.pdf&view=true. - Макрообъект. - ISBN 978-5-9967-1207-6.

2. Култыгин, О. П. Администрирование баз данных. СУБД MS SQL Server: [Электронный ресурс]: учеб. пособие / О. П. Култыгин. - М.: МФПА, 2012. - 232 с. - (Университетская серия). - Режим доступа: http://znanium.com/bookread.php?book=451114 - Загл. с экрана. - ISBN 978-5-4257-0026-1.

3. Ажмухамедов И.М. Основы организационно-правового обеспечения информационной безопасности: [Электронный ресурс]: учеб. пособие / И.М. Ажмухамедов, О.М. Князева. - СПб.: Издательский центр «Интермедия», 2017. – 264 с. - Режим доступа: https://ibooks.ru/product.php?productid=356930 - Загл. с экрана. - ISBN: 978-5-4383-0160-8.

4. Унижаев Н.В. Информационно-аналитическое обеспечение безопасности организации: [Электронный ресурс]: учеб. пособие / Н.В. Унижаев - СПб.: Издательский центр «Интермедия», 2018. – 408с. - Режим доступа: https://ibooks.ru/product.php?productid=356934. - Загл. с экрана. - ISBN: 978-5-4383-0158-5.

5. Царегородцев А.В. Методы и средства защиты информации в государственном управлении: [Электронный ресурс]: учеб. пособие / А.В. Царегородцев, М.М. Тараскин. - Москва: Проспект, 2017. - 208 с. - Режим доступа: https://ibooks.ru/product.php?productid=356008 . - Загл. с экрана. - ISBN: 978-5-392-20353-6.

6. Баркалов С.А. Информационная безопасность при управлении техническими системами: [Электронный ресурс]: учеб. пособие /, О.М. Барсуков, В.Е. Белоусов, К.В. Славнов. – СПб.: ИЦ «Интермедия», 2016. – 528с.: илл. - 208 с. - Режим доступа: https://ibooks.ru/product.php?productid=356935 - Загл. с экрана. - ISBN: 978-5-4383-0133-2.

в) Программное обеспечение и Интернет-ресурсы:

1. Журнал Information Security. Информационная безопасность [Электронный ресурс]: периодич. интернет-изд. – Режим доступа: http://www.itsec.ru/articles2/allpubliks – Загл. с экрана. Яз. рус.
2. Журнал «Безопасность информационных технологий» [Электронный ресурс]: периодич. интернет-изд. – Режим доступа: http://www.pvti.ru/articles_14.htm – Загл. с экрана. Яз. рус.
3. Журнал «Вопросы кибербезопасности» [Электронный ресурс]: периодич. интернет-изд. – Режим доступа: http://cyberrus.com/ – Загл. с экрана. Яз. рус.
4. «Журнал сетевых решений LAN»: [Электронный ресурс]: периодич. интернет-изд. URL: http://www.osp.ru/lan/ Издательство "Открытые системы. СУБД". – Режим доступа: http://www.osp.ru/os/ – Загл. с экрана. Яз. рус.
5. Государственная публичная научно-техническая библиотека России [Электронный ресурс] / – Режим доступа: http://www.gpntb.ru, свободный.– Загл. с экрана. Яз. рус.
6. Российская национальная библиотека. [Электронный ресурс] / – Режим доступа: http://www.nlr.ru. Яз. рус.
7. Безопасник [Электронный ресурс]. – Режим доступа: http://www.безопасник.рф .– Загл. с экрана. Яз. рус.
8. Компьтерра: все новости про компьютеры, железо, новые технологии, информационные технологии [Электронный ресурс]. – Периодическое электронное Интернет-издание – Режим доступа: http://www.computerra.ru/ – Загл. с экрана. Яз. рус.
9. ФСТЭК России [Электронный ресурс] – Режим доступа: http://fstec.ru/.– Загл. с экрана. Яз. рус.

9. Материально-техническое обеспечение дисциплины

Тип и название аудитории	Оснащение аудитории
Лекционная аудитория (ауд. 2124, ауд. 226, ауд. 365, ауд. 388 и т.д.)	Мультимедийные средства хранения, передачи и представления информации
Компьютерный класс (ауд. 372, ауд. 245, ауд. 247, ауд. 144, ауд. 142 и т.д.)	Персональные компьютеры с ПО: Операционная система MS Windows 7 (Microsoft Imagine Premium D-1227-18 от 08.10.2018 до 08.10.2021); Пакет MS Office (Microsoft Open License 42649837, бессрочная); Выход в Интернет и доступ в электронную информационно-образовательную среду университета.
Лаборатория программно-аппаратных средств защиты информации, ауд. 2124	**Система компьютерной защиты информации КриптоПро CSP.** Средство криптографической защиты информации «КриптоПро CSP» Версия 3.6 на одном рабочем месте MS Windows (Серийный номер: 3636C-Y0000- 01W74-WPDLF-QQBYU, бессрочная); Средство криптографической защиты информации «КриптоПро CSP» версии 3.6 на сервере MS Windows (Серийный номер: 36369-V0000- 02NGL-YN8P4- YNFR0, бессрочная); Средство криптографической защиты информации «КриптоПро CSP» Версия 3.6 на одном рабочем месте MS Windows (Серийный номер: 3636E-D0000- 01CHL-ZV2NZ-TXXDZ, бессрочная); Средство криптографической защиты информации «КриптоПро CSP» Версия 3.6 на одном рабочем месте MS (Серийный номер: 3636E-H0000- 01LB9-TFBF0- 9MPEX, бессрочная); Средство криптографической защиты информации «КриптоПро CSP» Версия 3.6 на одном рабочем месте MS Windows (Серийный номер: 36363-L0000- 01Z7X-AQ47B-CGF5M, бессрочная); Средство криптографической защиты информации «КриптоПро CSP» Версия 3.6 на одном рабочем месте MS Windows (Серийный номер: 36362-10000-01E6F- TTA6U-4BVAD, бессрочная); Средство криптографической защиты информации «КриптоПро CSP» Версия 3.6 на одном рабочем месте MS Windows (Серийный номер: 3636W-50000- 01CR0-4C5Y2-5WDH9, бессрочная); Средство криптографической защиты информации «КриптоПро CSP» Версия 3.6 на одном рабочем месте MS Windows (Серийный номер: 36364-R0000- 0136K-K81XR DLN6G, бессрочная); Средство криптографической защиты информации «КриптоПро CSP» Версия 3.6 на одном рабочем месте MS Windows (Серийный номер: 3636W-H0000- 01TAY-OLZOM-EQ0M6, бессрочная); Средство криптографической защиты информации «КриптоПро CSP» Версия 3.6 на одном рабочем месте MS Windows (Серийный номер: 3636U-V0000-0108W-CM6XF-H9763, бессрочная);

Тип и название аудитории	Оснащение аудитории
	Средство криптографической защиты информации «КриптоПро CSP» Версия 3.6 на одном рабочем месте MS Windows (Серийный номер: 3636W-Q0000- 01NKG-UD8N1-5MUHQ, бессрочная); Средство криптографической защиты информации «КриптоПро CSP» Версия 3.6 на одном рабочем месте MS Windows (Серийный номер: 3636V-K0000-01CNV-GFKKA-DDDVQ, бессрочная); Средство криптографической защиты информации «КриптоПро CSP» Версия 3.6 на одном рабочем месте MS Windows (Серийный номер: 3636M- 30000-01CCB- A5EQL-YH02R, бессрочная). Операционная система MS Windows 7 (Microsoft Imagine Premium D-1227-18 от 08.10.2018 до 08.10.2021).
Лаборатория радиомониторинга и контроля утечек информации, ауд. 226	Комплект учебного оборудования «Системы контроля доступа», «Системы видеонаблюдения».
Аудитории для самостоятельной работы (ауд. 132а): компьютерные классы; читальные залы библиотеки.	Персональные компьютеры с ПО: Операционная система MS Windows 7 (Microsoft Imagine Premium D-1227-18 от 08.10.2018 до 08.10.2021); Пакет MS Office 2007 (Microsoft Open License 42649837, бессрочная); Выход в Интернет и доступ в электронную информационно-образовательную среду университета.

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций и ПрООП ВО для специальности *10.05.03 Информационная безопасность автоматизированных систем. Специализация «Обеспечение информационной безопасности распределенных информационных систем».*