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)

ЗАЩИТА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

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	5
Семестр	9

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: зав.кафедрой ИиИБ, д.т.н., профессор
(должность, ученая степень, ученое звание)

_____ И.И. Баранкова /
(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

Целями изучения дисциплины «Защита программного обеспечения» являются: освоение технических средств защиты, нормативно-правовых документов и организационных методов в области обеспечения защиты от несанкционированного использования и копирования программного обеспечения; методов противодействия разрушению, нарушения целостности и достоверности программного обеспечения; частных политик информационной безопасности автоматизированной системы в соответствии с требованиями ФГОС ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем».

2. Место дисциплины в структуре образовательной программы подготовки специалиста

Дисциплина «Защита программного обеспечения» входит в вариативную часть блока 1 образовательной программы..

Для освоения дисциплины обучающиеся используют знания, умения и компетенции, сформированные в ходе изучения основных положений курсов «Безопасность операционных систем», «Техническая защита информации», «Разработка и эксплуатация защищенных автоматизированных систем», «Технология построения защищенных распределенных приложений», «Технологии и методы программирования».

Дисциплина является предшествующей для успешного выполнения научно-исследовательской работы и ВКР.

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

В результате освоения дисциплины «Защита программного обеспечения» обучающийся должен обладать следующими компетенциями:

Структурный элемент компетенции	Планируемые результаты обучения
ПК-10 способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности	
Знать	- Современные технологии программирования. - Области и особенности применения языков программирования высокого уровня; - Основные виды интегрированных сред разработки программного обеспечения. - Основные методы эффективного кодирования. - Способы обработки исключительных ситуаций; - Современные технологии и методы программирования, предназначенные для создания прикладных программ в защищенном исполнении.
Уметь	- Реализовывать на языке высокого уровня алгоритмы решения профессиональных задач; - Работать с основными средами интегрированной разработки программного обеспечения; - Проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения; - Реализовывать разработанную структуру классов для задач предметной области.
Владеть	- Навыками реализации алгоритмов на языках программирования высокого уровня; - Навыками пользования библиотеками прикладных программ для решения прикладных задач профессиональной области. - Технологиями программирования распределенных автоматизированных систем;

Структурный элемент компетенции	Планируемые результаты обучения
	- Способностью использовать языки, системы и инструментальные средства разработки автоматизированных систем.
ПК-27 способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	
Знать	– способы обработки исключительных ситуаций; современные технологии и методы программирования, предназначенные для создания прикладных программ; – Способы разработки политики безопасности распределенных ИС. – Нормативные документы по стандартизации и сертификации программной защиты. – Способы управления разработкой политики безопасности распределенных ИС. – Методы и средства анализа достаточности мер по обеспечению ИБ ПО
Уметь	– Разрабатывать частные политики безопасности распределенных ИС. – Проводить мониторинг и аудит защищенности ПО – Руководить разработкой и реализацией частных политики безопасности.
Владеть	– Методиками анализа политики безопасности. – Методиками разработки политики безопасности. – Методами анализа достаточности мер по обеспечению ИБ процессов создания и эксплуатации ПО
ПСК-7.4 способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах	
Знать	- принципы построения и функционирования, архитектуру, примеры реализаций современных систем управления базами данных; - основные модели данных, физическую организацию баз данных; - последовательность и содержание этапов проектирования баз данных;
Уметь	- разрабатывать и администрировать базы данных и интерфейсы прикладных программ к базам данных; - выделять сущности и связи предметной области; - выполнять запросы к базе данных; - нормализовывать отношения при проектировании реляционной базы данных; - создавать объекты базы данных;
Владеть	- методиками безопасной работы с БД с помощью современных образцов программных, технических средств; -в полной мере средствами администрирования БД в интегрированных средах СУБД.

Структура и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет **5** зачетных единиц **180** акад. часов, в том числе:

- контактная работа – 106,85 акад. часов:
  - аудиторная – 102 акад. часов;
  - внеаудиторная – 4,85 акад. часов
- самостоятельная работа – 37,45акад. часов;
- подготовка к экзамену – 35,7 акад. часов;

Форма аттестации:

- 9 семестр – экзамен

Раздел/ тема дисциплины	Семестр	Аудиторная		Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		Лекции	Практич. Занятия				
Раздел 1. Введение в теорию обеспечения безопасности программного обеспечения и данных							
Тема 1.1. Основные положения теории безопасности программ и данных. Угрозы безопасности программному обеспечению и данным. Теоретические основы дисциплины и терминология.	9	3	3/1И	2	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к практическому занятию	тестирование	ПК-10 з ПК-27 з ПСК-7.4 з
Тема 1.2 Основные принципы обеспечения безопасности программного обеспечения и данных. Технологическая и эксплуатационная безопасность программ	9	4	4/1И	2	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к практическому занятию	тестирование	ПК-10 зу ПК-27 зу ПСК-7.4 зу

Раздел/ тема дисциплины	Семестр	Аудиторная		Самостоятельная работа (в акад.	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент
		Лекции	Практич. Занятия				
Тема 1.3 Правовая и организационная поддержка процессов разработки и применения программного обеспечения. Стандарты и другие нормативные документы, регламентирующие защищенность программного обеспечения и обрабатываемой информации.	9	4	4/1И	2	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к контрольной работе; подготовка к практическому занятию	Тестирование, АКР-1	ПК-10 зу ПК-27 зу ПСК-7.4 зу
Итого по разделу		11	11/3И	6			
Раздел 2. Способы тестирования программного обеспечения при испытаниях его на технологическую безопасность							
Тема 2.1. Обобщенные способы анализа программных средств на предмет наличия (отсутствия) разрушающих программных средств.	9	4	4/1И	2	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к контрольной работе; подготовка к практическому занятию	Тестирование, АКР-2	ПК-10 з ПК-27 з ПСК-7.4 з
Тема 2.2. Построение программно-аппаратных комплексов для контроля технологической безопасности программного обеспечения и данных.	9	4	4/2И	4	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к контрольной работе; подготовка к практическому занятию; выполнение практического задания	Тестирование, АКР-3	ПК-10 зув ПК-27 зув ПСК-7.4 зув
Итого по разделу		8	8/3И	6			
Раздел 3. Методы и средства обеспечения							

Раздел/ тема дисциплины	Семестр	Аудиторная		Самостоятельная работа (в акад.	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент
		Лекции	Практич. Занятия				
целостности и достоверности используемого программного кода							
Тема 3.1. Методы защиты программ и данных от несанкционированных изменений. Проверка целостности программ и данных.	9	4	4/1И	2	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к контрольной работе; подготовка к практическому занятию	Тестирование, АКР-4	ПК-10 зув ПК-27 зув ПСК-7.4 зу
Тема 3.2. Схема подписи с верификацией по запросу. Примеры применения схемы подписи с верификацией по запросу.	9	4	4/2И	3	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к контрольной работе; подготовка к практическому занятию	Тестирование, АКР-5	ПК-10 зув ПК-27 зув ПСК-7.4 зу
Тема 3.3. Основные подходы к защите программного обеспечения от несанкционированного копирования.	9	4	4/1И	4	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к контрольной работе; подготовка к практическому занятию	Тестирование, АКР-6	ПК-10 зув ПК-27 зув ПСК-7.4 зу
Итого по разделу		12	12/4И	9			
Раздел 4. Администрирование и защита БД							

Раздел/ тема дисциплины	Семестр	Аудиторная		Самостоятельная работа (в акад.	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент
		Лекции	Практич. Занятия				
Тема 4.1 Понятия администрирование, привилегия, доступ. Виды пользователей и группы привилегий, соответствующие виду пользователя.	9	4	4/2И	2	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к контрольной работе; подготовка к практическому занятию	Тестирование, АКР-7	ПК-10 зув ПК-27 зув ПСК-7.4 зув
Тема 4.2 Программные и программно-аппаратные средства защиты БД	9	4	4/2И	4	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к практическому занятию	Тестирование,	ПК-10 зув ПК-27 зув ПСК-7.4 зув
Тема 4.3 Контроль доступа к данным. Управление привилегиями пользователей базы данных. Идентификация и аутентификация пользователя. Пароли.	9	4	4/4И	4	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к контрольной работе; подготовка к практическому занятию	Тестирование, АКР-8	ПК-10 зув ПК-27 зув ПСК-7.4 зув
Тема 4.4. Транзакционный подход к организации доступа к данным. Понятие SQL Injection. Виды уязвимостей, используемые атаками SQL Injection. Методы защиты от Injection.	9	4	4/2И	4	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к контрольной работе; подготовка к практическому занятию	Тестирование, АКР-9	ПК-10 зув ПК-27 зув ПСК-7.4 зув
Тема 4.5 Использование аудита БД. Аудит	9	4	4/2И	2,45	Подготовка к практическому занятию;	Тестирование,	ПК-10

Раздел/ тема дисциплины	Семестр	Аудиторная		Самостоятельная работа (в акад.	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент
		Лекции	Практич. Занятия				
системных событий. Системы обнаружения вторжений.					поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к контрольной работе; подготовка к практическому занятию	АКР-9	зув ПК-27 зув ПСК-7.4 зув
Итого по разделу		20	20/12И	16			
Подготовка к экзамену				35,7		**Промежуточная аттестация (экзамен)**	
Итого за семестр		**51**	**51/22И**	**73,15**		**Промежуточная аттестация (экзамен)**	
Итого по дисциплине		**51**	**51/22И**	**73,15**		**Промежуточная аттестация (экзамен)**	

5 Образовательные и информационные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины «Методы проектирования защищенных распределенных информационных систем» используются традиционная и модульно-компетентностная технологии.

Реализация компетентностного подхода предусматривает использование в учебном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

При проведении учебных занятий преподаватель обеспечивает развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств посредством проведения интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализа ситуаций , учета особенностей профессиональной деятельности выпускников и потребностей работодателей.

Формы учебных занятий с использованием традиционных технологий:

- ***обзорные лекции*** – для рассмотрения общих вопросов Информатики и информационных технологий, для систематизации и закрепления знаний;
- ***информационные*** – для ознакомления с техническими средствами реализации информационных процессов, со стандартами организации сетей, основными приемами защиты информации, и другой справочной информацией;
- ***Практическое занятие***, посвященное освоению конкретных умений и навыков по предложенному алгоритму.

Формы учебных занятий с использованием технологий проблемного обучения:

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

- ***проблемная*** - для развития исследовательских навыков и изучения способов решения задач.
- ***лекции с заранее запланированными ошибками*** – направленные на поиск обучающимися синтаксических и алгоритмических ошибок при решении алгоритмических и функциональных задач, с последующей диагностикой слушателей и разбором сделанных ошибок.
- ***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.
- ***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

Формы учебных занятий с использованием игровых технологий:

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

Технологии проектного обучения

- ***Творческий проект*** – учебно-познавательная деятельность обучающихся осуществляется в

рамках рамочного задания, подчиняясь логике и интересам участников проекта, жанру конечного результата (газета, фильм, праздник, издание, экскурсия, подготовка заданий конкурсов и т.п.).

- ***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).

Формы учебных занятий с использованием информационно-коммуникационных технологий:

- ***Лекция-визуализация*** – изложение содержания сопровождается презентацией (демонстрацией учебных материалов, представленных в различных знаковых системах, в т.ч. иллюстративных, графических, аудио- и видеоматериалов).
- ***Практическое занятие в форме презентации*** – представление результатов проектной или исследовательской деятельности с использованием специализированных программных сред.

- ***методы IT***
  - Подготовка и проведение практических работ по поиску информации в сетях. Задание критериев поиска информации. Работа с поисковыми системами университета и внешними ресурсами.
  - Подготовка и проведение лабораторных работ по архивации данных с целью дальнейшего использования в средствах телекоммуникационных технологий: электронной почте, чате, телеконференции т.д.
  - Организация доступа обучающихся к основным и дополнительным лекционным материалам с использованием клиент-серверных технологий (платформа e-Learning).
  - Использование электронных образовательных ресурсов для организации самостоятельной работы обучающихся. Разработка преподавателями кафедры авторских ЭОР, подготовка перечня и ориентация обучающихся на государственные образовательные интернет-ресурсы.
  - Использование в образовательном процессе электронных учебников, компьютерных обучающих систем, интерактивных упражнений.
  - Компьютерный практикум.
- ***работа в команде***
  - Разработка Web-проектов.
- ***case-study***
  - Разбор результатов тематических контрольных работ, анализ ошибок, совместный поиск вариантов рационального решения учебной проблемы.
- ***проблемное обучение***
  - Подготовка тематических рефератов, содержащих разделы, частично или полностью выносимые на самостоятельное изучение.
- ***учебная дискуссия***
  - Проведение семинаров, посвященных вопросам информатики, подготовка тематических презентаций по заданным темам, и дальнейший обмен взглядами по конкретной проблеме.
- ***использование тренингов***
  - Подготовка и проведение демонстрационных, тематических и итоговых компьютерных тестирований как в качестве локальных, так и внешних контрольных мероприятий.

6. Учебно-методическое обеспечение самостоятельной работы обучающихся

По дисциплине «Методы проектирования защищенных распределенных информационных систем» предусмотрена аудиторная и внеаудиторная самостоятельная работа обучающихся.

Аудиторная самостоятельная работа обучающихся предполагает решение контрольных задач на практических занятиях.

Аудиторная самостоятельная работа обучающихся на практических занятиях осуществляется под контролем преподавателя в виде решения задач и выполнения упражнений, которые определяет преподаватель для обучающегося

Внеаудиторная самостоятельная работа обучающихся осуществляется в виде изучения литературы по соответствующему разделу с проработкой материала; выполнения домашних заданий, подготовки к аудиторным контрольным работам и выполнения домашних заданий с консультациями преподавателя.

Примерные задания и вопросы по темам:

Перечень вопросов контрольных работ и тестирования по темам разделов 1-4:

1. Перечислите меры, используемые для защиты программных продуктов от несанкционированного использования.
2. Перечислите модули системы технической защиты ПО от несанкционированного использования. Кратко охарактеризуйте функции каждого из них.
3. Приведите примеры характеристик среды, к которым можно осуществить привязку ПО для обнаружения факта несанкционированного использования.
4. В чем достоинства и недостатки встроенных и пристыковочных систем защиты ПО?
5. На какие из модулей системы защиты ПО от несанкционированного использования обычно осуществляет атаку злоумышленник?
6. Перечислите требования к блоку сравнения характеристик среды.
7. В чем особенности атак злоумышленника на блок установки характеристик среды и блок ответной реакции?
8. Перечислите и охарактеризуйте базовые методы нейтрализации систем защиты ПО от несанкционированного использования.
9. Перечислите средства статического исследования ПО. Кратко охарактеризуйте их.
10. Перечислите средства динамического исследования ПО. Кратко охарактеризуйте их.
11. Перечислите основные WinAPI функции, которые может использовать злоумышленник для локализации кода защиты. В каких случаях злоумышленник попытается отлавливать каждую из этих функций?
12. Перечислите и охарактеризуйте базовые методы противодействия отладке программного обеспечения.
13. Перечислите и охарактеризуйте несколько триков для отладчиков реального и защищенного режимов. В чем их недостатки?
14. Перечислите и охарактеризуйте базовые методы противодействия дизассемблированию программного обеспечения.
15. Охарактеризуйте способ защиты от отладки, основанный на особенностях конвейеризации процессора.
16. Охарактеризуйте возможности противодействия отладке и дизассемблированию, основанные на использовании недокументированных инструкций и недокументированных возможностей процессора. В чем недостатки данных методов?
17. Охарактеризуйте шифрование кода программы как наиболее универсальный метод противодействия отладке и дизассемблированию ПО.
18. Дайте определение программы с потенциально опасными последствиями. Какие функции свойственны данным программам?

19. Перечислите основные классы программ с потенциально опасными последствиями. Дайте их сравнительную характеристику.
20. Что понимают под активизирующим событием? Перечислите основные виды активизирующих событий для РПВ.
21. Перечислите и охарактеризуйте основные модели взаимодействия прикладной программы и РПВ.
22. Опишите основные группы деструктивных функций, свойственных программным закладкам.
23. Какие механизмы защиты являются общими для ОС и БД (СУБД)?
24. Перечислите характерные для технологии БД требования по безопасности данных.
25. Чем отличается управление доступом от управления целостностью БД?
26. В чем заключается сходство и различие механизмов управления доступом к БД, использующих таблицы (матрицы) доступа и внешнюю схему БД?
27. Предложите способы выявления косвенного предоставления права доступа для систем с динамическим управлением доступом (на примере СУБД DB).
28. Перечислите нарушения целостности БД, связанные с параллельным выполнением транзакций.
29. Назовите достаточное условие сериализуемости расписания выполнения транзакций.
30. Перечислите способы, позволяющие избежать тупиковых ситуаций. Перечислите способы выхода из состояния клинча транзакций.
31. Перечислите уровни восстановления БД. В чем заключается сущность каждого уровня?
32. Защита программного обеспечения с помощью аппаратных ключей серии Guardant
33. Технологии аутентификации и шифрования. Реализация безопасной сетевой инфраструктуры для web-сервера.
34. Классификация firewall'ов и определение политики firewall'а.
35. Обеспечение безопасности web-серверов. Безопасность web-содержимого. Электронные цифровые сертификаты; SSL/TLS.

7. Оценочные средства для проведения промежуточной аттестации

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

Структурный элемент	Планируемые результаты обучения	Оценочные средства
ПК-10 способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности		
Знать	- Современные технологии программирования. - Области и особенности применения языков программирования высокого уровня; - Основные виды интегрированных сред	1. Перечислите меры, используемые для защиты программных продуктов от несанкционированного использования. 2. Перечислите модули системы технической защиты ПО от несанкционированного использования. Кратко охарактеризуйте функции каждого из них. 3. Приведите примеры характеристик среды, к которым можно осуществить привязку ПО для обнаружения факта несанкционированного использования.

мент Структурный	Планируемые результаты обучения	Оценочные средства
	разработки программного обеспечения. - Основные методы эффективного кодирования. - Способы обработки исключительных ситуаций; - Современные технологии и методы программирования, предназначенные для создания прикладных программ в защищенном исполнении.	4. В чем достоинства и недостатки встроенных и пристыковочных систем защиты ПО? 5. На какие из модулей системы защиты ПО от несанкционированного использования обычно осуществляет атаку злоумышленник? 6. Перечислите требования к блоку сравнения характеристик среды. 7. В чем особенности атак злоумышленника на блок установки характеристик среды и блок ответной реакции? 8. Перечислите и охарактеризуйте базовые методы нейтрализации систем защиты ПО от несанкционированного использования. 9. Перечислите средства статического исследования ПО. Кратко охарактеризуйте их. 10. Перечислите средства динамического исследования ПО. Кратко охарактеризуйте их. 11. Перечислите основные WinAPI функции, которые может использовать злоумышленник для локализации кода защиты. В каких случаях злоумышленник попытается отлавливать каждую из этих функций? 12. Перечислите и охарактеризуйте базовые методы противодействия отладке программного обеспечения. 13. Перечислите и охарактеризуйте несколько триков для отладчиков реального и защищенного режимов. В чем их недостатки? 14. Перечислите и охарактеризуйте базовые методы противодействия дизассемблированию программного обеспечения. 15. Охарактеризуйте способ защиты от отладки, основанный на особенностях конвейеризации процессора. 16. Охарактеризуйте возможности противодействия отладке и дизассемблированию, основанные на использовании недокументированных инструкций и недокументированных возможностей процессора. В чем недостатки данных методов? 17. Охарактеризуйте шифрование кода программы как наиболее универсальный метод противодействия отладке и дизассемблированию ПО. 18. Дайте определение программы с потенциально опасными последствиями. Какие функции свойственны данным программам? 19. Перечислите основные классы программ с потенциально опасными последствиями. Дайте их сравнительную характеристику.

Структурный элемент	Планируемые результаты обучения	Оценочные средства
		20. Что понимают под активизирующим событием? Перечислите основные виды активизирующих событий для РПВ. 21. Перечислите и охарактеризуйте основные модели взаимодействия прикладной программы и РПВ. 22. Опишите основные группы деструктивных функций, свойственных программным закладкам.
Уметь	- Реализовывать на языке высокого уровня алгоритмы решения профессиональных задач; - Работать с основными средами интегрированной разработки программного обеспечения; - Проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения; - Реализовывать разработанную структуру классов для задач предметной области.	**1.** Разработать алгоритм от несанкционированного доступа. Доступ к файлу данных по паролю. **2.** Разработать алгоритм и реализовать программу для защиты программ с помощью контрольного суммирования. **3.** Разработать алгоритм и реализовать программу защиты сопровождения: регистрация обращений**.** **4.** Разработать алгоритм и реализовать программу защиты программного обеспечения от несанкционированного доступа путем привязки ПО к ПК.
Владеть	- Навыками реализации алгоритмов на языках программирования высокого уровня; - Навыками пользования библиотеками прикладных программ для решения прикладных задач профессиональной области. - Технологиями программирования	1. Методикой привязки ПО для обнаружения факта несанкционированного использования. 2. Методикой противодействия дизассемблированию программного обеспечения. 3. Методикой определения разрушающих программных воздействий

Структурный элемент	Планируемые результаты обучения	Оценочные средства
	распределенных автоматизированных систем; - Способностью использовать языки, системы и инструментальные средства разработки автоматизированных систем.	
ПК-27 способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы		
Знать	– способы обработки исключительных ситуаций; современные технологии и методы программирования, предназначенные для создания прикладных программ; – Способы разработки политики безопасности распределенных ИС. – Нормативные документы по стандартизации и сертификации программной защиты. – Способы управления разработкой политики безопасности распределенных ИС. – Методы и средства анализа достаточности мер по обеспечению ИБ ПО	1. Аудит баз данных и его виды: стандартный, на основе значений, детализированный 2. Аудит администратора БД. 3. Обслуживание журнала аудита. 4. Обновления системы безопасности 5. Обслуживание базы данных Оптимизаторы БД. 6. Сбор статистики оптимизатора и управление ею. 7. Автоматический репозиторий рабочей нагрузки и управление им. 8. Монитор автоматической диагностики баз данных. 9. Диспетчер и консультанты БД. 10. Автоматические задачи обслуживания. 11. Предупреждения сервера, их типы и реагирование на них.
Уметь	– Разрабатывать частные политики безопасности распределенных ИС. – Проводить мониторинг и аудит защищенности ПО – Руководить разработкой и реализацией частных политики безопасности.	1. Провести анализ защищенности исходного кода ПО 2. Провести анализ защищенности ПО от дизассемблирования 3. Разработать частную политику для реализуемой БД 4. Провести детализованный аудит БД 5. Провести аудит транзакций реализуемой БД 6. Провести анализ разграничения доступа пользователей БД
Владе	– Методиками анализа	1. Методикой разработки частной политики реализуемой БД

Структурный элемент	Планируемые результаты обучения	Оценочные средства
ть	политики безопасности. – Методиками разработки политики безопасности. – Методами анализа достаточности мер по обеспечению ИБ процессов создания и эксплуатации ПО	2. Методикой анализа разграничения доступа пользователей БД 3. Методикой сбора данных транзакций БД 4. Методикой анализа защищенности исходного кода ПО 5. Методикой анализа защищенности ПО от дизассемблирования
ПСК-7.4 способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах		
Знать	- принципы построения и функционирования, архитектуру, примеры реализаций современных систем управления базами данных; - основные модели данных, физическую организацию баз данных; - последовательность и содержание этапов проектирования баз данных;	1. Какие механизмы защиты являются общими для ОС и БД (СУБД)? 2. Перечислите характерные для технологии БД требования по безопасности данных. 3. Чем отличается управление доступом от управления целостностью БД? 4. В чем заключается сходство и различие механизмов управления доступом к БД, использующих таблицы (матрицы) доступа и внешнюю схему БД? 5. Предложите способы выявления косвенного предоставления права доступа для систем с динамическим управлением доступом (на примере СУБД DB). 6. Перечислите нарушения целостности БД, связанные с параллельным выполнением транзакций. 7. Назовите достаточное условие сериализуемости расписания выполнения транзакций. 8. Перечислите способы, позволяющие избежать тупиковых ситуаций. Перечислите способы выхода из состояния клинча транзакций. 9. Перечислите уровни восстановления БД. В чем заключается сущность каждого уровня? 10. Защита программного обеспечения с помощью аппаратных ключей серии Guardant 11. Технологии аутентификации и шифрования. Реализация безопасной сетевой инфраструктуры для web-сервера. 12. Классификация firewall’ов и определение политики firewall’а. 13. Обеспечение безопасности web-серверов. Безопасность web-содержимого. Электронные цифровые сертификаты; SSL/TLS.
Уметь	- разрабатывать и администрировать базы данных и	**1.** Провести администрирование реализуемой БД **2.** Разработать защищенную авторизацию в БД **3.** Разработать запросы к БД в защищенном исполнение

Структурный элемент	Планируемые результаты обучения	Оценочные средства
	интерфейсы прикладных программ к базам данных; - выделять сущности и связи предметной области; - выполнять запросы к базе данных; - нормализовывать отношения при проектировании реляционной базы данных; - создавать объекты базы данных;	**4.** Реализовать защиту БД от SQL инъекций
Владеть	- методиками безопасной работы с БД с помощью современных образцов программных, технических средств; -в полной мере средствами администрирования БД в интегрированных средах СУБД.	1. Методикой разграничения прав работы пользователей реализуемой БД 2. Методикой выделения привилегий пользователей БД 3. Методикой реализации меток безопасности и принудительного контроля доступа 4. Методикой реализации домена безопасности БД

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

Промежуточная аттестация по дисциплине включает теоретические вопросы, позволяющие оценить уровень усвоения обучающимися знаний, и практические задания, выявляющие степень сформированности умений и владений, проводится в форме зачета и экзамена.

Показатели и критерии оценивания экзамена:

– на оценку **«отлично»** (5 баллов) – обучающийся демонстрирует высокий уровень сформированности компетенций, всестороннее, систематическое и глубокое знание учебного материала, свободно выполняет практические задания, свободно оперирует знаниями, умениями, применяет их в ситуациях повышенной сложности.

– на оценку **«хорошо»** (4 балла) – обучающийся демонстрирует средний уровень сформированности компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.

– на оценку **«удовлетворительно»** (3 балла) – обучающийся демонстрирует пороговый уровень сформированности компетенций: в ходе контрольных мероприятий допускаются ошибки,

проявляется отсутствие отдельных знаний, умений, навыков, обучающийся испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

– на оценку **«неудовлетворительно»** (2 балла) – обучающийся демонстрирует знания не более 20% теоретического материала, допускает существенные ошибки, не может показать интеллектуальные навыки решения простых задач.

– на оценку **«неудовлетворительно»** (1 балл) – обучающийся не может показать знания на уровне воспроизведения и объяснения информации, не может показать интеллектуальные навыки решения простых задач.

8. Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс]: Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - Режим доступа: http://znanium.com/bookread.php?book=405000. - Загл. с экрана. - ISBN 978-5-369-01178-2.

2. Бухтояров, В.В. Поддержка принятия решений при проектировании систем защиты информации: Монография / В.В. Бухтояров, В.Г. Жуков, В.В. Золотарев. - М.: НИЦ ИНФРА-М, 2014. - 131 с. – Режим доступа: http://znanium.com/bookread.php?book=445551 Заглавие с экрана.– ISBN 978-5-16-009516-6.

3. Проектирование информационных систем [Электронный ресурс]: Учебное пособие / В.В. Коваленко. - М.: Форум: НИЦ ИНФРА-М, 2014. - 320 с.- (Высшее образование). Режим доступа: http://znanium.com/bookread.php?book=473097 .– Заглавие с экрана. –ISBN 978-5-91134-549-5 .

б) Дополнительная литература:

1. Шаньгин, В.Ф. Информационная безопасность [Электронный ресурс] — М. : ДМК Пресс, 2014. — 702 с. Режим доступа: http://e.lanbook.com/view/book/50578/.– Заглавие с экрана.

2. Жук, А.П. Защита информации [Электронный ресурс]: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.- (Высшее образование: Бакалавриат; Магистратура). –Режим доступа: http://znanium.com/bookread.php?book=474838 .– Заглавие с экрана.– ISBN 978-5-369-01378-6.

в) **Интернет – ресурсы**:

1. Журнал Information Security. Информационная безопасность: периодич. интернет-изд. URL: http://www.itsec.ru/articles2/allpubliks – Загл. с экрана. Яз. рус.

2. Журнал «Вопросы кибербезопасности»: периодич. интернет-изд. URL: http://cyberrus.com/ – Загл. с экрана. Яз. рус.

3. Государственная публичная научно-техническая библиотека России [Электронный ресурс] – Режим доступа: http://www.gpntb.ru , свободный.– Загл. с экрана. Яз. рус.

4. Российская национальная библиотека. [Электронный ресурс] / –URL: http://www.nlr.ru. Яз. рус.

5. Безопасник [Электронный ресурс] – Режим доступа: http://www.безопасник.рф .– Загл. с экрана. Яз. рус.

6. 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.

7. ФСТЭК России [Электронный ресурс] – Режим доступа: http://fstec.ru/.– Загл. с экрана. Яз. рус.

9. Материально-техническое обеспечение дисциплины

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 - *Microsoft Imagine Premium D-1227-18 от 08.10.2018 до 08.10.2021* ; Пакет MS Office (Microsoft Word, Microsoft Excel, Microsoft Access) - *Microsoft Open License 42649837, бессрочная*; Архиватор 7zip - *GNU LGPL, бессрочная*; Система компьютерной математики MathCad - *43813518 D-1662-13 от 22.11.2013*; выход в Интернет.
Аудитории для самостоятельной работы (ауд.132а): компьютерные классы; читальные залы библиотеки	Персональные компьютеры с ПО: - Операционная система MS Windows - *Microsoft Imagine - Premium D-1227-18 от 08.10.2018 до 08.10.2021* ; - Пакет MS Office (Microsoft Word, Microsoft Excel, Microsoft Access) - *Microsoft Open License 42649837, бессрочная*; - Архиватор 7zip - *GNU LGPL, бессрочная*; - Выход в Интернет и с 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».*