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
В.Р. Храмшин

13.02.2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ЗАЩИТА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Направление подготовки (специальность)
10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль/специализация) программы
10.05.03 специализация N 8 "Разработка автоматизированных систем в защищенном исполнении"

Уровень высшего образования - специалитет

Форма обучения
очная

Институт/ факультет	Институт энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	5
Семестр	9

Магнитогорск
2024 год

Рабочая программа составлена на основе ФГОС ВО - специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем (приказ Минобрнауки России от 26.11.2020 г. № 1457)

Рабочая программа рассмотрена и одобрена на заседании кафедры Информатики и информационной безопасности
09.02.2024, протокол № 4

Зав. кафедрой _____ И.И. Баранкова

Рабочая программа одобрена методической комиссией ИЭиАС
13.02.2024 г. протокол № 4

Председатель _____ В.Р. Храмшин

Рабочая программа составлена:
зав. кафедрой ИиИБ, д-р техн. наук _____ И.И. Баранкова

Рецензент:
начальник отдела информационной
безопасности «КУБ» (АО) , _____ М.М. Близнецов

Лист актуализации рабочей программы

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2025 - 2026 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 2026 - 2027 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 2027 - 2028 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 2028 - 2029 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 2029 - 2030 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 2030 - 2031 учебном году на заседании кафедры Информатики и информационной безопасности

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

1 Цели освоения дисциплины (модуля)

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 (модуля) в структуре образовательной программы

Дисциплина Защита программного обеспечения входит в часть учебного плана формируемую участниками образовательных отношений образовательной программы.

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

Безопасность операционных систем

Технология построения защищенных распределенных приложений

Технологии и методы программирования

Методы выявления нарушений информационной безопасности

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

Обеспечение информационной безопасности критической информационной инфраструктурой

Производственная - научно-исследовательская работа

Производственная - преддипломная практика

Подготовка к сдаче и сдача государственного экзамена

Форензика

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

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

Код индикатора	Индикатор достижения компетенции
ПК-3 Способен анализировать причины возникновения компьютерных инцидентов	
ПК-3.1	Определяет причину и условия изменения программного обеспечения
ПК-3.2	Определяет принципы деления программного обеспечения на группы, их специфические свойства и взаимосвязь с компьютерной системой
ПК-3.3	Прогнозирует возможные пути развития новых видов компьютерных преступлений, правонарушений и инцидентов
ПК-5 Способен проводить аттестацию объектов на соответствие требованиям по защите информации	
ПК-5.1	Проводит аттестационные испытания объектов вычислительной техники на соответствие требованиям по защите информации
ПК-5.2	Оформляет материалы аттестационных испытаний на соответствие требованиям по защите информации
ПК-5.3	Оформляет аттестат соответствия объектов вычислительной техники требованиям по защите информации

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 4 зачетных единиц 144 акад. часов, в том числе:

– контактная работа – 57,2 акад. часов:

– аудиторная – 54 акад. часов;

– внеаудиторная – 3,2 акад. часов;

– самостоятельная работа – 51,1 акад. часов;

– в форме практической подготовки – 0 акад. час;

– подготовка к экзамену – 35,7 акад. час

Форма аттестации - 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. Введение в теорию обеспечения безопасности программного обеспечения и данных								
1.1 Основные положения теории безопасности программ и данных. Угрозы безопасности программному обеспечению и данным. Теоретические основы дисциплины и терминология.	9	1		2	3,1	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-3.1, ПК-3.2, ПК-3.3, ПК-5.1, ПК-5.2, ПК-5.3

1.2 Основные принципы обеспечения безопасности программного обеспечения и данных. Технологическая и эксплуатационная безопасность программ		1		2	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-3.1, ПК-3.2, ПК-3.3, ПК-5.1, ПК-5.2, ПК-5.3
1.3 Правовая и организационная поддержка процессов разработки и применения программного обеспечения. Стандарты и другие нормативные документы, регламентирующие защищенность программного обеспечения и обрабатываемой информации.		1		2	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-1	ПК-3.1, ПК-3.2, ПК-3.3, ПК-5.1, ПК-5.2, ПК-5.3
Итого по разделу		3		6	11,1			
2. Способы тестирования программного обеспечения при испытаниях его на технологическую безопасность								

2.1 Обобщенные способы анализа программных средств на предмет наличия (отсутствия) разрушающих программных средств.	9	1		2	5	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-3.1, ПК-3.2, ПК-3.3, ПК-5.1, ПК-5.2, ПК-5.3
2.2 Построение программно-аппаратных комплексов для контроля технологической безопасности программного обеспечения и данных.		1		2	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-3.1, ПК-3.2, ПК-3.3, ПК-5.1, ПК-5.2, ПК-5.3
Итого по разделу		2		4	9			
3. Методы и средства обеспечения целостности и достоверности используемого программного кода								

3.1 Методы защиты программ и данных от несанкционированных изменений. Проверка целостности программ и данных.	9	1		2	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-4	ПК-3.1, ПК-3.2, ПК-3.3, ПК-5.1, ПК-5.2, ПК-5.3
3.2 Схема подписи с верификацией по запросу. Примеры применения схемы подписи с верификацией по запросу.		1		2	5	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-3.1, ПК-3.2, ПК-3.3, ПК-5.1, ПК-5.2, ПК-5.3
3.3 Основные подходы к защите программного обеспечения от несанкционированного копирования.		2		2	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-3.1, ПК-3.2, ПК-3.3, ПК-5.1, ПК-5.2, ПК-5.3

Итого по разделу		4		6	13			
4. Администрирование и защита БД								
4.1 Понятия администрирование, привилегия, доступ. Виды пользователей и группы привилегий, соответствующие виду пользователя.	9	1		4	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-3.1, ПК-3.2, ПК-3.3, ПК-5.1, ПК-5.2, ПК-5.3
4.2 Программные и программно-аппаратные средства защиты БД		2		4	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-3.1, ПК-3.2, ПК-3.3, ПК-5.1, ПК-5.2, ПК-5.3
4.3 Контроль доступа к данным. Управление привилегиями пользователей базы данных. Идентификация и аутентификация пользователя. Пароли.		2		4	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-3.1, ПК-3.2, ПК-3.3, ПК-5.1, ПК-5.2, ПК-5.3

4.4 Транзакционный подход к организации доступа к данным. Понятие SQL Injection. Виды уязвимостей, используемые атаками SQL Injection. Методы защиты от Injection.		2		4	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-3.1, ПК-3.2, ПК-3.3, ПК-5.1, ПК-5.2, ПК-5.3
4.5 Использование аудита БД. Аудит системных событий. Системы обнаружения вторжений.		2		4	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-3.1, ПК-3.2, ПК-3.3, ПК-5.1, ПК-5.2, ПК-5.3
4.6 Подготовка к экзамену.						Подготовка к экзамену.	Экзамен	
Итого по разделу		9		20	18			
Итого за семестр		18		36	51,1		экзамен	
Итого по дисциплине		18		36	51,1		экзамен	

5 Образовательные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины «Защита программного обеспечения» 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.

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

Представлено в приложении 1.

7 Оценочные средства для проведения промежуточной аттестации

Представлены в приложении 2.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/537247 (дата обращения: 25.04.2024). – Режим доступа: по подписке.

2. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2024. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/539995 (дата обращения: 25.04.2024). – Режим доступа: по подписке.

3. Полищук, Ю. В. Базы данных и их безопасность : учебное пособие / Ю.В. Полищук, А.С. Боровский. — Москва : ИНФРА-М, 2024. — 210 с. — (Среднее профессиональное образование). - ISBN 978-5-16-016151-8. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2136720 (дата обращения: 25.04.2024). – Режим доступа: по подписке.

б) Дополнительная литература:

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2024. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/538066 (дата обращения: 25.04.2024).

2. Запечников, С. В. Криптографические методы защиты информации : учебник для вузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва : Издательство Юрайт, 2024. — 309 с. — (Высшее образование). — ISBN 978-5-534-02574-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/536453 (дата обращения: 25.04.2024).

3. Внуков, А. А. Защита информации в банковских системах : учебное пособие

для вузов / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2024. — 246 с. — (Высшее образование). — ISBN 978-5-534-01679-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/537248 (дата обращения: 25.04.2024).

МАКРООБЪЕКТЫ:

4. Мазнин, Д.Н. Сетевая защита информации. Лабораторный практикум : учебное пособие [для вузов] / Д. Н. Мазнин, И. И. Баранкова, У. В. Михайлова, М. В. Афанасьева ; 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://host.megaprolib.net/MP0109/Download/MObject/2400. - ISBN 978-5-9967-1605-0. - Текст : электронный. (дата обращения: 25.04.2024)

5. Баранков, В.В. Развертывание и настройка виртуальных сетей : учебное пособие [для вузов] / [сост.: В. В. Баранков, И. И. Баранкова, У. В. Михайлова, О. Б. Калугина] ; МГТУ. - Магнитогорск : МГТУ, 2019. - 1 электрон. опт. диск (CD-ROM). - URL: https://host.megaprolib.net/MP0109/Download/MObject/2388. - ISBN 978-5-9967-1305-9. - Текст : электронный. (дата обращения: 25.04.2024)

в) Методические указания:

1. Методические указания по выполнению практических работ по дисциплине «Защита программного обеспечения» (Приложение 3).

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия лицензии
7Zip	свободно распространяемое ПО	бессрочно
MariaDB	свободно распространяемое ПО	бессрочно
PostgreSQL	свободно распространяемое ПО	бессрочно
MS Office 2007 Professional	№ 135 от 17.09.2007	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
LibreOffice	свободно распространяемое ПО	бессрочно
MS Visual Studio Code	свободно распространяемое ПО	бессрочно
MS Visual Studio 2017 Community Edition	свободно распространяемое ПО	бессрочно
Adobe Reader	свободно распространяемое ПО	бессрочно

Браузер	свободно	бессрочно
Браузер Mozilla	свободно распространяе	бессрочно
FAR	свободно	бессрочно
Linux	свободно	бессрочно
Oracle Virtual	свободно распространяе	бессрочно
NotePad+	свободно	бессрочно
JetBrains PyCharm Community Edition	свободно распространяемое ПО	бессрочно
JetBrains IDEA Communi	свободно распространяемое ПО	бессрочно
MS Office	№ 135 от 17.09.2007	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Информационная система - Банк данных	https://bdu.fstec.ru/?ysclid=lujkqy7cnw630508962
Информационная система - Нормативные правовые акты, организационно-распоря дительные документы,	https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-tzi?ysclid=lujknksfy724757053
Архив научных журналов «Национальный	https://arch.neicon.ru/xmlui/
Международная реферативная и полнотекстовая	https://www.nature.com/siteindex
Международная база полнотекстовых	http://link.springer.com/
Федеральный образовательный портал	http://ecsocman.hse.ru/
Электронные ресурсы библиотеки МГТУ им.	https://host.megaprolib.net/MP0109/Web
Российская Государственная	https://www.rsl.ru/ru/4readers/catalogues/
Федеральное государственное бюджетное учреждение	URL: http://www1.fips.ru/
Поисковая система Академия Google	URL: https://scholar.google.ru/
Национальная информационно-аналитическая система –	URL: https://elibrary.ru/project_risc.asp
Электронная база периодических изданий	https://dlib.eastview.com/

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

Материально-техническое обеспечение дисциплины включает:

Лекционные аудитории:

- мультимедийные средства хранения, передачи и представления информации.

Учебные аудитории для проведения практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации:

- персональные компьютеры с ПО, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета;
- мультимедийные средства хранения, передачи и представления информации;
- комплекс тестовых заданий для проведения промежуточных и рубежных контролей.

Помещения для самостоятельной работы обучающихся:

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

Помещения для хранения и профилактического обслуживания учебного оборудования: шкафы для хранения учебно-методической документации, учебного оборудования и учебно-наглядных пособий.

Приложение 1

Учебно-методическое обеспечение самостоятельной работы обучающихся

По дисциплине «Защита программного обеспечения» 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.

Приложение 2

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
ПК-3 Способен анализировать причины возникновения компьютерных инцидентов		
ПК-3.1	Определяет причину и условия изменения программного обеспечения	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

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		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.

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
ПК-3.2	Определяет принципы деления программного обеспечения на группы, их специфические свойства и взаимосвязь с компьютерной системой	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. 5. Разграничить права работы пользователей реализуемой БД и программного обеспечения 6. Выделить привилегии пользователей БД. 7. Реализовать распределение меток безопасности и принудительного контроля доступа к программному обеспечению. 8. Произвести настройку домена безопасности БД.
ПК-3.3	Прогнозирует возможные пути развития новых видов компьютерных преступлений, правонарушений и инцидентов	1. Используя брандмауэр Windows настроить доступ приложения к локальной сети и интернет. 2. Используя встроенные средства Windows настроить доступ пользователя к программному обеспечению. 3. Настроить защиту от программ-шантажистов и провести оценку журнала событий Windows. 4. Используя встроенные средства Windows настроить доступ к программному обеспечению через доступ к папке.
ПК-5 Способен проводить аттестацию объектов на соответствие требованиям по защите информации		
ПК-5.1	– Проводит аттестационные испытания объектов вычислительной техники на соответствие требованиям по защите информации	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.
ПК-5.2	Оформляет материалы аттестационных испытаний на соответствие требованиям по защите информации	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.

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		7. Провести администрирование реализуемой БД. 8. Разработать защищенную авторизацию в БД. 9. Разработать запросы к БД в защищенном исполнение. 10. Реализовать защиту БД от SQL инъекций. 11. Настроить защиту программного обеспечения с применением дистанционного администрирования.
ПК-5.3	Оформляет аттестат соответствия объектов вычислительной техники требованиям по защите информации	1. Разработать частную политику администрирования реализуемой БД. 2. Провести анализ разграничения доступа пользователей БД. 3. Провести анализ сбора данных транзакций БД используя встроенные средства СУБД. 4. Используя встроенные средства Windows, провести анализ исходного кода ПО. 5. Используя встроенные утилиты администрирования Windows провести анализ событий по указанному программному обеспечению.

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.

Приложение 3

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.