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)

АНАЛИЗ БЕЗОПАСНОСТИ 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	4,5
Семестр	8,9

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: ст.преподаватель кафедры ИиИБ, к. т.н.
(должность, ученая степень, ученое звание)

_____ / М.В. Коновалов /
(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

Общей целью дисциплины «Анализ безопасности программного обеспечения» является повышение исходного уровня владения информационными технологиями, достигнутого на предыдущей ступени образования, и овладение студентами необходимым и достаточным уровнем профессиональных компетенций в соответствии с требованиями ФГОС ВО по специальности «Информационная безопасность автоматизированных систем». Специальными целями дисциплины «Анализ безопасности программного обеспечения» являются:

- изучить контрольно-испытательные и логико-аналитические методы анализа безопасности программного обеспечения и способы обеспечения надежности программ для контроля их технологической безопасности;
- освоить способы оценки эффективности систем защиты программного обеспечения и технологии разработки систем программно-технической защиты

программного обеспечения.

2.Место дисциплины в структуре образовательной программы специалиста

Дисциплина «Анализ безопасности программного обеспечения» входит в вариативную часть блока №1 образовательной программы.

Для изучения дисциплины необходимы знания, умения и навыки, сформированные в результате освоения предыдущих дисциплин «Информатика», «Организация ЭВМ и вычислительных систем», «Техническая защита информации», «Программно-аппаратные средства обеспечения информационной безопасности», «Моделирование систем и процессов защиты информации», «Безопасность операционных систем», «Методы выявления нарушений информационной безопасности, аттестация АИС», «Технология построения защищенных распределенных приложений», «Методы проектирования защищенных распределенных информационных систем», «Организационное и правовое обеспечение информационной безопасности», «Сети и системы передачи информации», «Техническая защита информации», «Основы информационной безопасности», «Безопасность сетей ЭВМ».

Данная дисциплина необходима для последующего успешного выполнения научно-исследовательской работы, прохождения государственной итоговой аттестации и выполнения ВКР.

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

Структурный элемент компетенции	Планируемые результаты обучения
ПК-15. Способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем	
Знать:	- Нормативные документы по метрологии, стандартизации и сертификации программных средств защиты. - подходы к проведению сертификации информационной безопасности программного обеспечения;
Уметь:	- составлять регламент испытаний информационной безопасности программного обеспечения
Владеть:	- навыками применения специализированного ПО для проведения мероприятий при сертификации средств защиты информации автоматизированных систем;
ПК-17. Способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	
Знать:	- перечень инструментов для проведения мониторинга защищенности информации; - базовый функционал инструментов для проведения мониторинга защищенности информации;
Уметь:	- применять технические средства для проведения мониторинга беспроводных сетей; - применять технические средства для проведения мониторинга проводных сетей построенных на основе неуправляемых коммутаторов;
Владеть:	- навыками работы с специализированным программным обеспечением для проведения мониторинга защищенности информации в автоматизированной системе;

Структурный элемент компетенции	Планируемые результаты обучения
ПК-24. Способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	
Знать:	- методы повышения уровня безопасности за счет настройки прав доступа к ресурсам автоматизированной системы;
Уметь:	- выполнять работы по оптимизации схем управления автоматизированной системой; - выявлять узлы автоматизированной системы, не обеспечивающие требуемый уровень информационной безопасности;
Владеть:	- навыками определения возможных векторов атаки на автоматизированную систему;
ПСК-7.3. Способностью проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем	
Знать:	- Способы обработки исключительных ситуаций; -Методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем. -наиболее распространённые точки для несанкционированного входа в распределенную систему;
Уметь:	- проводить анализ уязвимостей распределённой системы; - получать несанкционированный доступ к ресурсам распределенной системы;
Владеть:	- навыками противодействия внешним атакам на распределенную информационную сеть;

4.Структура и содержание дисциплины «Анализ безопасности программного обеспечения**»**

Общая трудоемкость дисциплины составляет 5 зачетные единицы 180 часов:
– контактная работа – 89,2 акад. часов:
– аудиторная – 85 акад. часов;
– внеаудиторная – 4,1 акад. часов;
–самостоятельная работа – 55,3 акад. часов;
– подготовка к экзамену – 35,7 акад. часов
– вид аттестации – зачет, экзамен

Раздел дисциплины	Сем.	Аудиторная контактная работа			Самостоятельная работа	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	практика	лаб. работа				
Модуль 1 Теоретические и формальные методы доказательства правильности программ и их спецификаций.								
Тема. 1.1. Языки формальной спецификации программ. Валидация сценариев требований.	8	2	2/1,5	2	2,1	Подбор, описание, экспертная оценка сайтов Интернет, разработка глоссария к теме.	семинарское занятие;	ПК-15 зув ПК-17 зув ПК-24 зув ПСК-7.3 зув
Тема 1.2. Методы анализа структур программ. Верификация и валидация программ. Метод верификации композиции правильных компонентов	8	3	3/1,5	3	3	Подбор, описание, экспертная оценка сайтов Интернет, разработка глоссария к теме.	Семинарское занятие, устный опрос	ПК-15 зув ПК-17 зув ПК-24 зув ПСК-7.3 зув
Модуль 2 Контрольно-испытательные и логико-аналитические методы анализа безопасности программного обеспечения.								
Тема 2.1. Проблемы анализа безопасности программного обеспечения. Основные угрозы безопасности программного обеспечения.	8	3	3/1,5	3	3	Создание тестовой АС, ее конфигурация. Отслеживания действий пользователей АС.	Семинарское занятие, устный опрос	ПК-15 зув ПК-17 зув ПК-24 зув ПСК-7.3 зув
Тема 2.2. Алгоритмические и программные закладки.	8	3	3/1,5	3	4	Конфигурация прав пользователей АС		ПК-15 зув ПК-17 зув ПК-24 зув ПСК-7.3 зув
Модуль 3. Методы и средства анализа безопасности программ								
Тема 3.1. Лексический и синтаксический верификационный анализ, семантический анализ программ. Верификация моделей программ методом model checking.	8	3	3/1,5	3	4	Подбор, описание, экспертная оценка сайтов Интернет	устный опрос	ПК-15 зув ПК-17 зув ПК-24 зув ПСК-7.3 зув
Тема 3.2. Логика дерева вычислений: формализм для представления свойств живости и безопасности, алгоритмы верификации	8	3	3/1,5	3	4	Установка и настройка дистрибутива Kali Linux 2.	проектные работы.	ПК-15 зув ПК-17 зув ПК-24 зув ПСК-7.3 зув
Итого за семестр		17	17/9	17	20,1		Промежуточная аттестация (зачет)	
Модуль 4. Способы обеспечения надежности программ для контроля их технологической безопасности.								
Тема 4.1. Процессы обеспечения функциональной безопасности программных продуктов в стандартах IEC 61508:1-6: 1998-2000, ISO 15408:1999 93, ISO 13335: 1-5: 1998.	9	2	2/1,5		5,2	Настройка коммутатора на зеркалирование траффика на заданный узел. Зеркалирование трафика посредством ARP-инъекций	Защита проекта, устный опрос	ПК-15 зув ПК-17 зув ПК-24 зув ПСК-7.3 зув
Тема 4.2. Методы идентификации программ и их характеристик. Способы оценки подобия целевой и исследуемой программ с точки зрения наличия программных дефектов.	9	3	3/1,5		6	Конфигурирование патернов активности при помощи средств дистрибутива Kali Linux	Защита проекта, устный опрос	ПК-15 зув ПК-17 зув ПК-24 зув ПСК-7.3 зув
Модуль 5. Анализ средств и этапы преодоления систем защиты программного обеспечения.								
Тема 5.1. Методы защиты программ от исследования.	9	3	3/1,5		6	Анализ радиочастот для выявления каналов занятых исследуемой беспроводной сетью. Выполнение атаки на сеть сцелью получения	Защита проекта, устный опрос	ПК-15 зув ПК-17 зув ПК-24 зув ПСК-7.3 зув

						хедшейка. Подбор хэша.		
Тема 5.2. Технологии разработки систем программно-технической защиты программного обеспечения. Этапы проектирования и разработки систем программно-технической защиты программного обеспечения.	9	3	3/1,5		6	Анализ активности на радиочастотах занятых беспроводной сетью	Защита проекта, устный опрос	ПК-15 зув ПК-17 зув ПК-24 зув ПСК-7.3 зув
Модуль 6. Оценка эффективности систем защиты программного обеспечения.								
Тема 6.1. Критерии оценки: стойкость к исследованию/взлому; отказоустойчивость (надёжность);	9	3	3/1,5		6	Анализ HTML кода. Проверка простейших ошибок при конфигурировании страницы авторизации	Защита проекта, устный опрос	ПК-15 зув ПК-17 зув ПК-24 зув ПСК-7.3 зув
Тема 6.2. Критерии оценки: независимость от конкретных реализаций операционных систем; совместимость; неудобства для конечного пользователя программного обеспечения; побочные эффекты; стоимость; доброкачественность.	9	3	3/1,5		6	Применение основных типов SQL-инжекции для получения доступа данных авторизации	Защита проекта, устный опрос	ПК-15 зув ПК-17 зув ПК-24 зув ПСК-7.3 зув
Итого за семестр		17	17/9		35,2			
Итого по курсу:		34	34/18	17	55,3	Экзамен		

5. Образовательные и информационные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины «теория информации» 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;
- лекции-визуализации – для наглядного представления способов решения алгоритмических и функциональных задач, визуализации результатов решения задач;
- Семинар.
- 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 лабораторных 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 «Анализ безопасности 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 обучающихся.

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.

Примерный индивидуальные домашние задания

Модуль 1. Теоретические и формальные методы доказательства правильности программ и их спецификаций

1.Дайте определение формальной спецификации программного обеспечения.

2. Назовите категории классификации спецификаций программного обеспечения.

3. Определите основные понятия формальной спецификации VDM.

4. Определите основные базовые элементы спецификации RAISE.

5. Сравните математические понятия методов VDM и RAISE.

6. Определите цель и структуру концепторного языка.

7. Назовите формальные методы доказательства правильности программного обеспечения и приведите их короткую аннотацию.

8. Определите понятия пред- и постусловий, аксиом и утверждений программного обеспечения.

9. Опишите, как проходит процесс доказательства правильности программного обеспечения, заданной спецификацией.

10. В чем проблемы проведения доказательства правильности программного обеспечения с помощью формальных методов?

11. Приведите отличие техники формального доказательства правильности программного обеспечения от символьного выполнения программ?

Модуль 2 Контрольно-испытательные и логико-аналитические методы анализа безопасности программного обеспечения.

1. Дайте определение верификации и валидации программного обеспечения.

2. В чем суть композиции верифицированных программ?

3. Расскажите о международном проекте по верификации программного обеспечения.

4. Перечислите контрольно-испытательные и логико-аналитические методы анализа безопасности программного обеспечения.

5. Какие бывают проблемы анализа безопасности программного обеспечения?

6. Назовите основные угрозы безопасности программного обеспечения.

7. Что такое алгоритмические и программные закладки программного обеспечения?

Модуль 3. Методы и средства анализа безопасности программ

1. Приведите классификацию методов и средств анализа безопасности программ.

2. Как используют лексический, синтаксический и семантический верификационный анализ для анализа безопасности программного обеспечения?

3. Как делается верификация моделей программ методом model checking?

4. Опишите логику дерева вычислений: формализм для представления свойств

живости и безопасности, алгоритмы верификации.

5. Опишите технологии создания алгоритмически безопасных процедур.

6. Какие бывают методы создания самотестирующихся и самокорректирующихся программ?

7. Опишите создание безопасного программного обеспечения на базе методов теории конфиденциальных вычислений.

Модуль 4. Способы обеспечения надежности программ для контроля их технологической безопасности.

1. Как делается защита программ и забывающее моделирование на RAM-машинах?

2. Какие вы знаете способы обеспечения надежности программ для контроля их технологической безопасности?

3. Перечислите процессы обеспечения функциональной безопасности программных продуктов в международных стандартах IEC и ISO.

4. Назовите методы идентификации программ и их характеристик.

5. Какие вы знаете способы оценки подобия целевой и исследуемой программ с точки зрения наличия программных дефектов?

Модуль 5. Анализ средств и этапы преодоления систем защиты программного обеспечения.

1. Охарактеризуйте анализ средств и этапы преодоления систем защиты программного обеспечения.

2. Перечислите и опишите методы защиты программ от исследования.

3. Опишите технологии разработки систем программно-технической защиты программного обеспечения.

4. Назовите этапы проектирования и разработки систем программно-технической защиты программного обеспечения.

5. Как делается оценка эффективности систем защиты программного обеспечения?

6. Какие вы знаете критерии оценки стойкости к исследованию или взлому программного обеспечения?

Модуль 6. Оценка эффективности систем защиты программного обеспечения.

1. Укажите критерии устойчивости программного обеспечения к исследованию и взлома.

2. Укажите критерии отказоустойчивости и надежности программного обеспечения

3. Укажите критерии оценки независимости программного обеспечения от конкретных реализаций операционных систем.

4. Укажите критерии оценки совместимости программного обеспечения.

5. Укажите критерии оценки графического интерфейса пользователя программного обеспечения.

6. Укажите критерии оценки побочных эффектов программного обеспечения.

7. Укажите критерии оценки стоимости программного обеспечения.

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
ПК-15. Способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем		
Знать	- Нормативные документы по метрологии, стандартизации и сертификации программных средств защиты. - подходы к проведению сертификации информационной безопасности программного обеспечения;;	1. Дайте определение формальной спецификации программного обеспечения. 2. Назовите категории классификации спецификаций программного обеспечения. 3. Определите основные понятия формальной спецификации VDM. 4. Определите основные базовые элементы спецификации RAISE. 5. Сравните математические понятия методов VDM и RAISE. 6. Определите цель и структуру концепторного языка. 7. Назовите формальные методы доказательства правильности программного обеспечения и приведите их короткую аннотацию. 8. Определите понятия пред- и постусловий, аксиом и утверждений программного обеспечения. 9. Опишите, как проходит процесс доказательства правильности программного обеспечения, заданной спецификацией.
Уметь	- составлять регламент испытаний информационной безопасности программного обеспечения	По представленному исходному коду программного обеспечения составить регламент испытаний.
Владеть	- навыками применения специализированного ПО для проведения мероприятий при сертификации средств защиты информации автоматизированных систем;	Дизасемблировать EXE-файл и выполнить анализ его внутренней структуры. Выполнить анализ занимаемой EXE-файлом оперативной памяти с целью определения адресов ячеек, в которых храниться заданные параметры.
ПК-17. Способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации		

Знать	- перечень инструментов для проведения мониторинга защищенности информации; - базовый функционал инструментов для проведения мониторинга защищенности информации;	1. В чем проблемы проведения доказательства правильности программного обеспечения с помощью формальных методов? 2. Приведите отличие техники формального доказательства правильности программного обеспечения от символьного выполнения программ? 3. Дайте определение верификации и валидации программного обеспечения. 4. В чем суть композиции верифицированных программ? 5. Расскажите о международном проекте по верификации программного обеспечения. 6. Перечислите контрольно-испытательные и логико-аналитические методы анализа безопасности программного обеспечения. 7. Какие бывают проблемы анализа безопасности программного обеспечения? 8. Назовите основные угрозы безопасности программного обеспечения. 9. Что такое алгоритмические и программные закладки программного обеспечения? 10. Приведите классификацию методов и средств анализа безопасности программ.
Уметь	- применять технические средства для проведения мониторинга беспроводных сетей; - применять технические средства для проведения мониторинга проводных сетей построенных на основе неуправляемых коммутаторов;	Определить протокол, используемый для авторизации участников сети. Выполнить атаку Pixie Dust. Определить причины по которым атака прошла успешно. Предложить меры по увеличению защищенности устройства. Выполнить атаку на роутер с авторизацией по протоколу WPA2. Определить причины по которым атака прошла успешно. Предложить меры по увеличению защищенности устройства.
Владеть	- навыками работы с специализированным программным обеспечением для проведения мониторинга защищенности информации в автоматизированной системе;	Провести комплексный тест выбранного узла при помощи инструментов дистрибутива Kali Linux 2.
ПК-24. Способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности		

Знать	- методы повышения уровня безопасности за счет настройки прав доступа к ресурсам автоматизированной системы;	1. Управление учетными записями пользователей. 2. Мониторинг процессов и приложений 3. Аудит событий в локальной системе 4. Объекты групповой политики (GPO). Создание. Редактирование. Хранение. 5. Сетевая информационная система NIS (NIS+) и ее конфигурирование. 6. Доступ к удаленным компьютерам 7. Виртуальные частные сети 8. Выбор режима проверки подлинности. 9. Авторизация пользователей. 10. Системные процедуры администрирования учетных записей Windows. 11. Системные процедуры администрирования учетных записей SQL Server.
Уметь	- выполнять работы по оптимизации схем управления автоматизированной системой; - выявлять узлы автоматизированной системы, не обеспечивающие требуемый уровень информационной безопасности;	1. На виртуальной машине по управление ОС Linux настроить iptable. 2. Настроить шаблон по которому весь трафик с заданного IP проходящий через порт 23 будет записан в файл. 3. При помощи утилиты Metasploit выполнить анализ узлов сети.
Владеть	- навыками определения возможных векторов атаки на автоматизированную систему;	Проанализировать конфигурацию узла автоматизированной системы и определить какие параметры конфигурации узла снижают его защищенность.
ПСК-7.3. Способностью проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем		

Знать	- Способы обработки исключительных ситуаций; -Методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем. -наиболее распространённые точки для несанкционированного входа в распределенную систему;	1.Как делается верификация моделей программ методом model checking? 2. Опишите логику дерева вычислений: формализм для представления свойств живости и безопасности, алгоритмы верификации. 3. Опишите технологии создания алгоритмически безопасных процедур. 4. Какие бывают методы создания самотестирующихся и самокорректирующихся программ? 5. Опишите создание безопасного программного обеспечения на базе методов теории конфиденциальных вычислений. 6. Как делается защита программ и забывающее моделирование на RAM-машинах? 7. Какие вы знаете способы обеспечения надежности программ для контроля их технологической безопасности? 8. Перечислите процессы обеспечения функциональной безопасности программных продуктов в международных стандартах IEC и ISO. 9. Назовите методы идентификации программ и их характеристик.
Уметь	- проводить анализ уязвимостей распределённой системы; - получать несанкционированный доступ к ресурсам распределенной системы;	При помощи утилиты Nmap провести тест заданного узла. Определить операционную систему сервера. Используемые протоколы и порты. Используя данные DNS определить связанные ресурсы. Провести их тест.
Владеть	- навыками противодействия внешним атакам на распределенную информационную сеть;	На Web сервере сконфигурировать авторизацию таким образом, чтобы сделать применение утилиты Hydra неэффективной. Разработать скрипт выполняющий проверку входной переменной для SQL – запроса. Если содержание переменной не корректно вывести соответствующее предупреждение.

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.

Критерии оценки для получения зачета

«зачтено» – обучающийся показывает средний уровень сформированности компетенций.

«не зачтено» – результат обучения не достигнут, обучающийся не может показать знания на уровне воспроизведения и объяснения информации, не может показать интеллектуальные навыки решения простых задач, не может показать знания на уровне

воспроизведения и объяснения информации.

Экзамен по данной дисциплине проводится в компьютерном классе по экзаменационным билетам, каждый из которых включает 1 теоретический вопрос и 2 практических задания.

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)

Основная литература

1. Аверченков, В.И. Аудит информационной безопасности [Электронный ресурс] : учебное пособие / В.И. Аверченков. — Электрон. дан. — Москва : ФЛИНТА, 2011. — 269 с. — Режим доступа: https://e.lanbook.com/book/44799. — Загл. с экрана.
2. Аникин, Д.В. Информационная безопасность и защита информации [Электронный ресурс] : учебное пособие / Д.В. Аникин. — Электрон. дан. — Санкт-Петербург : ИЭО СПбУТУиЭ, 2011. — 269 с. — Режим доступа: https://e.lanbook.com/book/63950. — Загл. с экрана.

Дополнительная литература:

1. Каратунова, Н. Г. Защита информации. Курс лекций [Электронный ресурс] : Учебное пособие / Н. Г. Каратунова. - Краснодар: КСЭИ, 2014. - 188 с. - Режим доступа: http://www.znanium.com.–Заглавие с экрана.
2. Барнс, К. Защита от хакеров беспроводных сетей [Электронный ресурс] / К. Барнс, Т. Боутс, Д. Лойд, Э. Уле. — Электрон. дан. — Москва : ДМК Пресс, 2005. — 480 с. — Режим доступа: https://e.lanbook.com/book/1119. — Загл. с экрана.

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 «Безопасность информационных технологий» : периодич. интернет-изд. URL: http://www.pvti.ru/articles_14.htm – Загл. с экрана. Яз. рус.
3. Журнал «Вопросы кибербезопасности»: периодич. интернет-изд. URL: http://cyberrus.com/ – Загл. с экрана. Яз. рус.
4. «Журнал сетевых решений LAN»: периодич. интернет-изд. URL:

http://www.osp.ru/lan/ Издательство "Открытые системы. СУБД". URL: 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] / –URL: http://www.nlr.ru. Яз. рус.
7. Компьтерра: все новости про компьютеры, железо, новые технологии, информационные : периодич. интернет-изд. URL: http://www.computerra.ru/ – Загл. с экрана. Яз. рус.
8. http://www.безопасник.рф

9. Материально-техническое обеспечение дисциплины(модуля)

Тип и название аудитории	Оснащение аудитории
Лекционная аудитории 282, 374, 388	Мультимедийные средства хранения, передачи и представления информации
Лаборатория радиомониторинга и контроля утечек информации, ауд. 226	Комплекс радиомониторинга «Касандра К-6» и «Касандра К-21» с диапазоном рабочих частот от 0,009 до 6000 МГц в расширенной комплектации с исполнением в ударопрочном кейсе. Комплект учебного оборудования «Системы мониторинга информационной безопасности».
Компьютерные классы 372-1-5	Персональные компьютеры под управление ОС Windows 7 (Microsoft Imagine Premium D-1227-18 от 08.10.2018 до 08.10.2021) с пакетом MS Office 2007 (Microsoft Open License 42649837), выходом в Интернет и с доступом в электронную информационно-образовательную среду университета
Аудитории для самостоятельной работы: компьютерные классы 132; читальные залы, библиотеки.	Персональные компьютеры под управление ОС Windows 7 (Microsoft Imagine Premium D-1227-18 от 08.10.2018 до 08.10.2021) с пакетом MS Office 2007 (Microsoft Open License 42649837), выходом в Интернет и с доступом 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».