МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«Национальный исследовательский ядерный университет «МИФИ»

Саровский физико-технический институт -

филиал федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский ядерный университет «МИФИ»

(**СарФТИ НИЯУ МИФИ**)

ФИЗИКО-ТЕХНИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра Цифровых технологий

УТВЕРЖДАЮ:

Декан ФТФ, д.ф.-м.н.

_____ А.К. Чернышев

«____» _____ 2023г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Технологии защиты информации и оценка соответствия

наименование дисциплины

Направление подготовки (специальность)	09.04.02 "Информационные системы и технологии"
Наименование образовательной программы	Инновационные технологии комплексной автоматизации и сквозного управления жизненным циклом
Квалификация (степень) выпускника	магистр
Форма обучения	очная

Программа одобрена на заседании кафедры

протокол № от 2023 г.

Зав. кафедрой ЦТ

_____ Кривошеев О.В.

«____» _____ 2023 г.

г. Саров, 2023 г.

Программа переутверждена на 202____/202____учебный год с изменениями в соответствии с семестровыми учебными планами академических групп ФТФ на 202____/202_____ учебный год.

Заведующий кафедрой ЦТ Кривошеев О.В.

Программа переутверждена на 202____/202____учебный год с изменениями в соответствии с семестровыми учебными планами академических групп ФТФ на 202____/202_____ учебный год.

Заведующий кафедрой ЦТ Кривошеев О.В.

Программа переутверждена на 202____/202____учебный год с изменениями в соответствии с семестровыми учебными планами академических групп ФТФ на 202____/202_____ учебный год.

Заведующий кафедрой ЦТ Кривошеев О.В.

Программа переутверждена на 202____/202____учебный год с изменениями в соответствии с семестровыми учебными планами академических групп ФТФ на 202____/202_____ учебный год.

Заведующий кафедрой ЦТ Кривошеев О.В.

Семестр	В форме практической подготовки	Трудоемкость, кред.	Общий объем курса, час.	Лекции, час.	Практич. занятия, час.	Лаборат. работы, час.	СРС, час.	КР/ КП	Форма(ы) контроля, экз./зач./ЗсО/
2	18	3	108	14	6	12	40	0	Э
ИТОГО	**18**	**3**	**108**	**14**	**6**	**12**	**40**	**0**	**36**

АННОТАЦИЯ

Дисциплина направлена на формирование у студентов профессиональных компетенций в области анализа уязвимостей и сертификации программного обеспечения. В ходе обучения у студентов формируются профессионально-ориентированные навыки, позволяющие применять на практике полученные знания в области практического решения задач анализа уязвимостей и процесса сертификации.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Цель изучения дисциплины – заключается в подготовке специалистов, разбирающихся в современных подходах к анализу уязвимостей, понимающих процессы сертификации программного обеспечения на основе передовых технологий, способных грамотно анализировать проблему и вырабатывать рекомендации по ее решению.

Задачи дисциплины:

– сформировать чёткое представление о процессах разработки безопасного ПО, процессах сертификации ПО по требованиям безопасности информации, ключевых технологиях, значимости процесса сертификации;

– студент должен знать предпосылки, нормативную и техническую базы, тенденции в области информационной безопасности, передовой отечественный и зарубежный опыт в данной области;

– должен знать ключевые технологии, составляющие основу анализа уязвимостей программного и программно-аппаратного обеспечения;

– сформировать представление об основных проблемах при анализе уязвимостей, путях их решения;

– должен знать особенности общих методологических подходов в области информационной безопасности и анализе уязвимостей, ключевые понятия информационной безопасности, процессов анализа уязвимостей и сертификации;

– должен уметь анализировать возможности и целесообразность применения ключевых компонентов процесса анализа уязвимостей;

– иметь комплексное представление о факторах, оказывающих негативное влияние на анализ уязвимостей и процесс сертификации в целом;

– сформировать представление о подходах к анализу уязвимостей и процессу сертификации.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

«Технологии защиты информации и оценка соответствия» является дисциплиной профиля «Инновационные технологии комплексной автоматизации и сквозного управления жизненным циклом» ООП по направлению 09.04.02 «Информационные системы и технологии».

Дисциплина направлена на формирование у студентов профессиональных компетенций в области анализа уязвимостей и сертификации программного обеспечения. В ходе обучения у студентов формируются профессионально-ориентированные навыки, позволяющие применять на практике полученные знания в области практического решения задач анализа уязвимостей и процесса сертификации.

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
УК-6 Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	З-УК-6 Знать: методики самооценки, самоконтроля и саморазвития с использованием подходов здоровьесбережения У-УК-6 Уметь: решать задачи собственного личностного и профессионального развития, определять и реализовывать приоритеты совершенствования собственной деятельности; применять методики самооценки и самоконтроля; применять методики, позволяющие улучшить и сохранить здоровье в процессе жизнедеятельности В-УК-6 Владеть: технологиями и навыками управления своей познавательной деятельностью и ее совершенствования на основе самооценки, самоконтроля и принципов самообразования в течение всей жизни, в том числе с использованием здоровьесберегающих подходов и методик
УКЦ-1 Способен решать исследовательские, научно-технические и производственные задачи в условиях неопределенности, в том числе выстраивать деловую коммуникацию и организовывать работу команды с использованием цифровых ресурсов и технологий в цифровой среде	З-УКЦ-1 Знать современные цифровые технологии, используемые для выстраивания деловой коммуникации и организации индивидуальной и командной работы У-УКЦ-1 Уметь подбирать наиболее релевантные цифровые решения для достижения поставленных целей и задач, в том числе в условиях неопределенности В-УКЦ-1 Владеть навыками решения исследовательских, научно-технических и производственных задач с использованием цифровых технологий
УКЦ-2 Способен к самообучению, самоактуализации и саморазвитию с использованием раз-	З-УКЦ-2 Знать основные цифровые платформы, технологи и интернет ресурсы используемые при онлайн обучении

личных цифровых технологий в условиях их непрерывного совершенствования	У-УКЦ-2 Уметь использовать различные цифровые технологии для организации обучения В-УКЦ-2 Владеть навыками самообучения, самооактуализации и саморазвития с использованием различных цифровых технологий

Профессиональные компетенции в соответствии с задачами и объектами (областями знаний) профессиональной деятельности:

Задача профессиональной деятельности (ЗПД)	**Объект или область знания**	**Код и наименование профессиональной компетенции**	**Код и наименование индикатора достижения профессиональной компетенции**
проектный			
проектно-исследовательская деятельность в области информационных технологий	цифровизация и комплексная автоматизация производств, управление сквозным жизненным циклом изделий, информационные процессы, технологии, системы и сети, их инструментальное (программное, техническое, организационное) обеспечение	ПК-3.1 Способен управлять научно-исследовательскими проектами в области ИТ малого и среднего уровня сложности, проектировать структуру и этапы жизненного цикла информационных систем и технологий в различных областях профессиональной деятельности Профессиональный стандарт «06.016. Руководитель проектов в области информационных технологий»	З-ПК-3.1 Знать: особенности управления научно- исследовательскими проектами, методы разработки информационных систем и технологий в различных областях профессиональной деятельности. У-ПК-3.1 Уметь: применять современные средства управления и разработки научно- исследовательских проектов, определять основные направления и этапы работ. В-ПК-3.1 Владеть: методиками оценки эффективности разработки и проектирования структуры и этапов жизненного цикла информационных систем и технологий в различных областях профессиональной деятельности.
		ПК-3.2 Способен обеспечивать управление работами по сопровождению и	З-ПК-3.2 Знать: состав технической документации, особенности документиро-

		модификации информационных систем и составлению технической документации и отчетности при решении задач профессиональной деятельности Профессиональный стандарт «06.015. Специалист по информационным системам»	вания взадачах сопровождения и модификации информационных систем. У-ПК-3.2 Уметь: управлять работами по модификации прикладных информационных систем при решении задач профессиональной деятельности. В-ПК-3.2 Владеть: навыками оформления отчетной документации на всех этапах разработки информационной системы.

3. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 3 ЗЕТа, 108 часов. Дисциплина читается на 1 курсе, 2 семестре.

№ п/п	Раздел учебной дисциплины	Недели	Виды учебной деятельности, включая СРС и трудоемкость (в часах)				Текущий контроль успеваемости *(неделя, форма)*	Аттестация раздела *(неделя, форма)*	Максимальный балл за раздел *
			Лекции	Практ. занятия/ семинары	Лабораторные работы	СРС			
2 семестр									
1.	Раздел 1. Обеспечение безопасности информации	1	2	0	0	5	Устный опорос		2
2.	Раздел 2. Моделирование угроз	2-4	2	2	4	10	Устный опорос		3
3.	Раздел 3. Тестирование функций безопасности								
4.	Раздел 4. Требования доверия к безопасности. Подготовка к проведению испытаний	5	2	0	0	5	Устный опорос		4

5.	Раздел 5. Анализ архитектуры	6	2	0	0	5	Устный опорос		4
6.	Раздел 6. Анализ уязвимостей по открытым источникам	7-9	2	2	4	5	Устный опорос		3
7.	Раздел 7. Статический анализ	10-11	2	2	0	5	Устный опорос		4
8.	Раздел 8. Динамическое тестирование	12-13	2	0	4	5	Устный опорос		10
9.	Итого работа в семестре		14	6	12	40			30
10.	Итоговая контрольная работа								20
11.	Зачет								0 - 50
12.	Итого за 2 семестр:								100

4.1. СОДЕРЖАНИЕ РАЗДЕЛОВ УЧЕБНОЙ ДИСЦИПЛИНЫ

Раздел 1. Обеспечение безопасности информации.

Вводная часть. Обеспечение безопасности информации. Понятие информации, подходы к защите информации. Понятие автоматизированной и информационной систем. Средства защиты информации, защищенные средства. Понятие сертификации, виды сертификационных испытаний. Процессы безопасной разработки, производства и технической поддержки.

Раздел 2. Моделирование угроз.

Моделирование угроз автоматизированных систем. Методический документ «Методика оценки угроз безопасности информации». Моделирование угроз при разработке защищенного ПО. Определение негативных последствий. Источники угроз. Определение актуальных угроз, актуального нарушителя.

Раздел 3. Тестирование функций безопасности.

Представление о методах и средствах защиты информации. Функциональные требования безопасности информации. Подходы к функциональному тестированию. Программа и методика испытаний.

Раздел 4. Требования доверия к безопасности. Подготовка к проведению испытаний.

Понятие поверхности атаки. Представление о преобразованиях исходного кода в процессе компиляции. Понятие кросс-компиляторов, транспиляторов, интерпретаторов, managed-кода. Особенности сертификации интерпретаторов и виртуальных машин. Настройка среды функционирования. Представление о контрольной и тестовой сборках

объекта оценки. Установка объекта оценки и контроль системных вызовов. Проведение антивирусного контроля при сборке объекта оценки.

Раздел 5. Анализ архитектуры.

Выявление потенциально опасных возможностей. Выявление архитектурных уязвимостей, нарушение технологии безопасного использования заимствованного кода. Уязвимости конфигурации. Применяемые методы при анализе архитектуры (мониторинг активности, анализ документации, извлечение информации из исполняемого кода, сканирование интерфейсов). Использование аутентификационных данных в исходных текстах. Формальная модель безопасности.

Раздел 6. Анализ уязвимостей по открытым источникам.

Идентификация уязвимостей по открытым источникам. Идентификация потенциальных уязвимостей. Тестирование на проникновение. Анализ сборочной среды на наличие негативного влияния.

Раздел 7. Статический анализ.

Синтаксис и семантика, типовые конструкции языков программирования. Понятие уязвимости, НДВ, программной закладки. Базы данных уязвимостей. Статические анализаторы, минимальные требования в зависимости от уровня доверия.

Раздел 8. Динамическое тестирование.

Подходы к фаззинг-тестированию, инструментирование, мутационный и генерационный фаззинг, написание обёрток, фаззинг программно-аппаратных изделий, фаззинг синтетических модулей. Формирование тестовых наборов данных. Определение условий завершения фаззинг-тестирования. Инструменты фаззинг-тестирования. Системное тестирование.

4.2. ПЛАН ПРАКТИЧЕСКИХ ЗАНЯТИЙ.

Занятие 1. Написание МУ, корректировка ЗБ. Тестирование прикладного приложения по ЗБ

Занятие 2. Использование инструментов Kali Linux.

Занятие 3. Статический анализ исходных текстов.

4.3. ПЛАН ЛАБОРАТОРНЫХ ЗАНЯТИЙ

Занятие 1. Тестирование приложения, разработка задания по безопасности.

Занятие 2. Проведение тестирования на проникновение.

Занятие 3. Фаззинг уязвимого приложения.

4. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В соответствии с требованиями ОС НИЯУ МИФИ по направлению 09.04.02 "Информационные системы и технологии" реализация компетентностного подхода предусматривает широкое использование в учебном процессе активных и интерактивных форм проведения занятий (деловых игр, разбор конкретных ситуаций и др.) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков студентов. В рамках учебного курса студенты работают с лекциями и рекомендованной литературой, готовятся к тестированию, выполняют домашние задания. В процессе подготовки студенты используют информационные источники, размещенные в сети Интернет (официальные сайты, веб-порталы, тематические форумы и телекоммуникации), электронные учебники и учебно-методические пособия, обучающие мультимедийные компакт-диски.

Преподавание дисциплины ведется с применением следующих видов образовательных технологий:

1. Информационно-коммуникационные технологии.
2. Работа в команде/работа в малой группе.
3. Проблемное обучение.
4. Опережающая самостоятельная работа.
5. Метод проблемного изложения.

Формы организации учебного процесса:

1. Лекция.
2. Практическое занятие.
3. Лабораторная работа.
4. Самостоятельная работа студентов.
5. Научно-исследовательская работа.

Содержание дисциплины имеет как теоретическую, так и практическую направленность. Следовательно, преподавание этого курса основывается на тесной связи достижений теории и практики и сопровождается получением практических навыков и умений в области цифровых технологий.

В связи с этим изучение курса предполагает сочетание таких взаимодополняющих форм занятий как лекция, практическое занятие, лабораторная работа, самостоятельная работа с научными и учебно-методическими источниками.

Лекционный материал освещает основные методологические подходы в области сертификации средств защиты информации и защищенного ПО по требованиям ФСТЭК

России. В процессе изложения лекционного материала применяются лекции-информации, проблемные лекции, лекции-конференции, информационно-коммуникативные технологии, электронные средства обучения (презентации, опорные конспекты, «облачные» образовательные материалы).

Практические занятия проводятся методом дискуссии, обсуждения докладов, проведения научно-практической конференции, круглых столов. Использование интерактивных форм обучения (деловые и ролевые игры) позволяет сформировать и развить практические умения и навыки.

Лабораторные занятия позволяют получить необходимые навыки в использовании основных инструментов, применяемых в процессе проведения анализа уязвимостей и процессе сертификации.

5. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ.

При изучении дисциплины предусматриваются следующие виды контроля:

- текущий;
- рубежный;
- итоговый (экзамен).

Оценочными средствами *текущего* контроля успеваемости студентов являются устный опрос и контрольная работа.

Рубежный контроль преследует цель выработать у студентов потребность в систематической работе по освоению теоретического материала дисциплины.

Итоговый контроль проводится после завершения обучения студентов дисциплины в виде экзамена.

Фонд оценочных средств по дисциплине обеспечивает проверку освоения планируемых результатов обучения (компетенций и их индикаторов) посредством мероприятий текущего, рубежного и промежуточного контроля по дисциплине.

5.1. Паспорт фонда оценочных средств по дисциплине

Связь между формируемыми компетенциями и формами контроля их освоения представлена в следующей таблице:

Раздел	Темы занятий	Компетенция	Индикаторы освоения	Текущий контроль, неделя
Семестр 2				
Раздел 1	Тема 1. Обеспечение безопасности информации	УК-6, УКЦ-1, УКЦ-2, ПК-3.1	З-УК-6;У-УК-6; В-УК-6	УО-2
	Тема 2. Моделирование угроз		З-УКЦ-1; У-УКЦ-1; В-УКЦ-1	УО - 4
	Тема 3. Тестирование функций безопасности		З-УКЦ-2; У-УКЦ-2; В-УКЦ-2	УО - 5
	Тема 4. Требования доверия к безопасности. Подготовка к проведению испытаний		З-ПК-3.1; У-З-ПК-3.1;В-ПК-3.1	УО-7
Рубежный контроль		УК-6, УКЦ-1, УКЦ-2, ПК-3.1	З-УК-6;У-УК-6; В-УК-6	Контр-8
			З-УКЦ-1; У-УКЦ-1; В-УКЦ-1	
			З-УКЦ-2; У-УКЦ-2; В-УКЦ-2	
			З-ПК-3.1; У-З-ПК-3.1;В-ПК-3.1	
Раздел 2	Тема 5. Анализ архитектуры	ПК-3.1, ПК-3.2	З-ПК-3.1;У- ПК-3.1; В- ПК-3.1	УО - 6
	Тема 6. Анализ уязвимостей по открытым источникам		З- ПК-3.2; У- ПК-3.2; В- ПК-3.2	Реф - 14
	Тема 7. Статический анализ			
	Тема 8. Динамическое тестирование			
Рубежный контроль		ПК-3.1, ПК-3.2	З-ПК-3.1;У- ПК-3.1; В- ПК-3.1	Тест – 15 (16)
			З- ПК-3.2; У- ПК-3.2; В- ПК-3.2	
Промежуточная аттестация		УК-6, УКЦ-1, УКЦ-2. ПК-3.2, ПК-3.1	З-УК-6;У-УК-6; В-УК-6	**Экзамен**
			З-УКЦ-1; У-УКЦ-1; В-УКЦ-1	
			З-УКЦ-2; У-УКЦ-2; В-УКЦ-2	
			З-ПК-3.1; У-З-ПК-3.1;В-ПК-3.1	
			З- ПК-3.2; У- ПК-3.2; В- ПК-3.2	

5.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности,

характеризующие этапы формирования компетенций в процессе освоения образовательной программы

Лекция 1:

1. Что значит термин «автоматизированная система»?
2. В чём разница между средством защиты информации и защищенным средством?
3. Объясните необходимость сертификации.
4. Перечислите основные системы сертификации, их области действия.
5. Перечислите виды сертификационных испытаний в системе сертификации ФСТЭК России, МО России.
6. Какие процессы необходимо внедрять при разработке безопасного ПО?

Лекция 2-3:

1. На что распространяется действие методического документа «Методика оценки угроз безопасности информации»?
2. План действий при моделировании угроз безопасности информации автоматизированных систем.
3. Какие виды нарушителей следует определить при моделировании угроз?
4. Какие существуют источники угроз?
5. На какие документы следует ориентироваться при написании модели угроз защищенного ПО?
6. Какие выделяются профили средств защиты информации?
7. На что необходимо ориентироваться при сертификации средства защиты, не имеющего профиля защиты?
8. Какие следует использовать входные данные при разработке программы и методики испытаний?
9. Что необходимо предпринять при отсутствии в сертифицируемом средстве нескольких функций из профиля защиты?
10. Сколько существуют классов защиты информации?
11. Поставьте в соответствие степень конфиденциальности информации и классы защиты.

Лекция 4:

1. Что включается в поверхность атаки?
2. Какие существуют преобразования в процессе компиляции?
3. Какие преобразования бинарного кода в процессе компиляции необходимо проверять на этапе ручного анализа?

4. Что такое транспилятор?

5. Особенности сертификации managed-кода и кода, написанного на языках программирования, использующих виртуальные машины и интерпретаторы.

6. Настройка среды функционирования при проведении сертификации.

7. Объясните, зачем необходима контрольная сборка? Контрольная компиляция и компоновка?

8. Зачем необходим контроль сетевого трафика во время компиляции ОО?

9. Приведите пример ПО, используемого для контроля сетевого трафика.

10. Что такое тестовая сборка?

11. Опишите особенности установки объекта оценки во время проведения сертификационных испытаний.

12. Зачем необходим контроль системных вызовов во время установки ОО?

13. Приведите пример ПО, используемого для контроля системных вызовов.

Лекция 5:

1. Как производится выявление потенциально опасных возможностей ПО при анализе архитектуры?

2. На основании чего производится выявление уязвимостей конфигурации?

3. Какие автоматизированные методы применяются на этапе анализа архитектуры?

4. Когда необходимо доказательство формальной модели безопасности?

Лекция 6:

1. Зачем необходим анализ уязвимостей по открытым источникам?

2. Какие источники рекомендуется использовать при анализе известных уязвимостей по открытым источникам?

3. Опишите основные достоинства и недостатки перечисленных ранее ресурсов.

4. Какие источники рекомендуется использовать при анализе потенциальных уязвимостей по открытым источникам?

5. В чём разница подходов при поиске известных и потенциальных уязвимостей?

6. Зачем необходимо тестирование на проникновение?

7. Опишите основные подходы к проведению тестирования на проникновение.

8. Что из себя представляет анализ сборочной среды на наличие негативного влияния?

9. Как проводить анализ негативного влияния сборочной среды в случае анализа бинарного кода методом «чёрного ящика»?

Лекция 7:

1. В чём разница синтаксического и семантического анализа?

2. Что такое «уязвимость»? Что такое НДВ? Что такое «Программная закладка»?
3. В чём разница между этими понятиями?
4. Какие существуют базы данных уязвимостей?
5. Зачем необходимы статические анализаторы?
6. Какие существуют требования к статическим анализаторам?
7. Что используют статические анализаторы в качестве входных данных?
8. Что получается в результате работы статического анализатора?

Лекция 8:

1. Какие подходы существуют к фаззинг-тестированию?
2. Зачем необходимо инструментирование?
3. Какие подходы существуют к инструментированию?
4. Способы получения качественных входных данных.
5. Какие ситуации способны выявлять современные фаззеры «из коробки»?
6. Зачем необходим сбор покрытия при проведении фаззинг-тестирования?
7. Нужен ли сбор покрытия в реальном времени? Зачем?
8. Мутационный и генерационный фаззинг. Необходимость генерационного фаззинга.
9. Зачем используется подход с написанием обёрток исследуемых функций?
10. Подходы к фаззингу программно-аппаратных изделий.
11. Определение условий завершения фаззинг-тестирования.
12. Основные инструменты фаззинг-тестирования.
13. Фаззинг managed-кода.
14. Подходы к проведению системного тестирования.

6.2 План самостоятельной работы студентов

Цели самостоятельной работы студентов:

– научить студентов элементарным формам представления результатов теоретических научных исследований в письменном виде;

– сформировать единые правила оформления исследования и библиографического списка

– использовать в работе и анализировать научную (первоисточники: монографии, статьи и др.), нормативно-методическую, учебную и справочную литературу;

– формулировать актуальность и значимость самостоятельного изучения нормативно-правовых документов;

– выделять цели, задачи, определять место и роль выбранной темы в рамках изучаемой дисциплины:

– учить анализировать, делать обобщения и выводы по исследуемому источнику.

Самостоятельная работа студентов в изучении дисциплины заключается:

– в подготовке и дополнении текстов лекций по темам дисциплины;

– подготовке к практическим занятиям (изучение теоретического материала по темам курса с использованием текста лекций и рекомендуемой литературы; выполнении индивидуальных заданий практических занятий);

– в выполнении лабораторных занятий.

Темы для подготовки рефератов

1. Определение поверхности атаки.
2. Преобразования бинарного кода в процессе компиляции. Методы анализа.
3. Подходы к сертификации транспилируемого исходного кода. Статический анализ, фаззинг-тестирование.
4. Подходы к сертификации кода, написанного на языке программирования, использующего виртуальную машину для исполнения.
5. Подходы к сертификации бинарного кода, использующего модификацию исполняемого кода в real-time.
6. Подходы к сертификации исполняемого кода BIOS.
7. Способы извлечения информации из исполняемого кода.
8. Анализ влияния системы автоматизации сборки на безопасность объекта оценки. Методы оценки.
9. Анализ влияния системы автоматизации сборки, способного исказить результаты испытаний. Методы оценки.
10. Методы поиска программных закладок и недекларированных возможностей.
11. Подходы к фаззинг-тестированию программно-аппаратных средств защиты информации.
12. Методы инструментации при проведении фаззинг-тестирования.
13. Отладочные аллокаторы. Необходимость. Основные подходы к разработке.
14. Кастомные санитайзеры. Необходимость. Основные подходы к разработке.
15. Методы разработки доверенного компилятора.

16. Методы поиска скрытых каналов по памяти в программном обеспечении.
17. Методы поиска скрытых каналов по времени в программном обеспечении.
18. Методы поиска статистических скрытых каналов в программном обеспечении.

Примерные вопросы к экзамену

1.Межсетевые экраны. Функции безопасности. Принципы работы.

2.Системы антивирусной защиты. Функции безопасности. Принципы работы.

3.Системы контроля накопителей. Функции безопасности. Принципы работы.

4.Системы обнаружения вторжений. Функции безопасности. Принципы работы.

5.Операционные системы. Функции безопасности. Принципы работы.

6.Средства доверенной загрузки. Функции безопасности. Принципы работы.

7.Моделирование угроз автоматизированной системы. Основные этапы.

8.Разработка безопасного ПО. Подходы к сертификации серийных изделий.

9.Подготовка испытательного стенда при проведении сертификации.

10. Определение поверхности атаки ОО. Различия по уровням доверия.
11. Методы, применяемые при анализе архитектуры.
12. Фаззинг-тестирование. Основные подходы. Получение входных данных
13. Фаззинг-тестирование. Мутационный и генерационный фаззинг.
14. Поиск известных уязвимостей по открытым источникам. Основные источники.
15. Поиск потенциальных уязвимостей по открытым источникам. Основные источники.
16. Поиск уязвимостей по открытым источникам. Уязвимости архитектуры. Уязвимости конфигурации.
17. Тестирование на проникновение.
18. Статический анализ. Понятия уязвимости, НДВ, программной закладки.

5.3. Шкалы оценки образовательных достижений

Рейтинговая оценка знаний является интегральным показателем качества теоретических и практических знаний и навыков студентов по дисциплине и складывается из оценок, полученных в ходе текущего контроля и промежуточной аттестации.

Результаты текущего контроля и промежуточной аттестации подводятся по шкале балльно-рейтинговой системы.

Шкала каждого контрольного мероприятия лежит в пределах от 0 до установленного максимального балла включительно. Итоговая аттестация по дисциплине оценивается по

100-балльной шкале и представляет собой сумму баллов, заработанных студентом при выполнении заданий в рамках текущего и промежуточного контроля.

Итоговая оценка выставляется в соответствии со следующей шкалой:

<table>
<tr><th>Сумма баллов</th><th>Оценка по 4-ех балльной шкале</th><th>Оценка ECTS</th><th>Требования к уровню освоению учебной дисциплины</th></tr>
<tr><td>90-100</td><td>5 – «отлично»</td><td>A</td><td>Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, использует в ответе материал монографической литературы.</td></tr>
<tr><td>85-89</td><td rowspan="3">4 – «хорошо»</td><td>B</td><td rowspan="3">Оценка «хорошо» выставляется студенту, если он твёрдо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.</td></tr>
<tr><td>75-84</td><td>C</td></tr>
<tr><td>70-74</td><td rowspan="2">D</td></tr>
<tr><td>65-69</td><td rowspan="2">3 – «удовлетворительно»</td><td rowspan="2">Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала.</td></tr>
<tr><td>60-64</td><td>E</td></tr>
<tr><td>Ниже 60</td><td>2 – «неудовлетворительно»</td><td>F</td><td>Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.</td></tr>
</table>

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

а) основная литература:

1. ГОСТ Р 56939-2016 ЗИ. Разработка безопасного программного обеспечения. Общие требования.

2. Выписка из Требований по безопасности информации, утвержденных приказом ФСТЭК России от 2 июня 2020 г. N 76.

3. Методический документ "Методика оценки угроз безопасности информации", утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.

4. Профиль защиты систем обнаружения вторжений уровня сети четвертого класса.

5. Профиль защиты систем обнаружения вторжений уровня узла четвертого класса.

6. Профиль защиты систем обнаружения вторжений уровня сети пятого класса.

7. Профиль защиты систем обнаружения вторжений уровня узла пятого класса.

8. Профиль защиты средств антивирусной защиты типа «А» четвертого класса.

9. Профиль защиты средств антивирусной защиты типа «Б» четвертого класса.

10. Профиль защиты средств антивирусной защиты типа «В» четвертого класса.

11. Профиль защиты средств антивирусной защиты типа «Г» четвертого класса.

12. Профиль защиты средства доверенной загрузки уровня платы расширения четвертого класса.

13. Профиль защиты средства доверенной загрузки уровня базовой системы ввода-вывода четвертого класса.

14. Профиль защиты средства доверенной загрузки уровня загрузочной записи пятого класса.

15. Профиль защиты средств контроля отчуждения (переноса) информации со съемных машинных носителей информации четвертого класса.

16. Профиль защиты средств контроля подключения съемных машинных носителей информации четвертого класса.

17. Профиль защиты межсетевых экранов типа «А» четвертого класса.

18. Профиль защиты межсетевых экранов типа «Б» четвертого класса.

19. Профиль защиты межсетевых экранов типа «В» четвертого класса.

20. Профиль защиты межсетевых экранов типа «Г» четвертого класса.

21. Профиль защиты межсетевых экранов типа «Д» четвертого класса.

22. ГОСТ Р 58143-2018. Детализация анализа уязвимостей программного обеспечения в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045.

Часть 1. Использование доступных источников для идентификации потенциальных уязвимостей.

23. ГОСТ Р 58143-2018. Детализация анализа уязвимостей программного обеспечения в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045. Часть 2. Тестирование проникновения.

24. ГОСТ Р 56545-2015 Защита информации. Уязвимости информационных систем. Правила описания уязвимостей.

25. ГОСТ Р 56546-2015 ЗИ. Уязвимости информационных систем. Классификация уязвимостей информационных систем

26. Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. Семь безопасных информационных технологий / Под. ред. А.С.Маркова. М.: ДМК Пресс, 2017. 224 с.

27. Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. - М.: ДМК Пресс, 2013. - 474 с.

28. Саттон М., Грин А., Амини П. — Fuzzing: исследование уязвимостей методом грубой силы. – Пер. с англ. – СПб.: Символ-Плюс, 2009. – 560 с., ил.

29. Эриксон Дж. — Хакинг. Искусство эксплойта, 2-е издание. - Пер. С англ. - СПб.: Символ-Плюс, 2010. - 512 с., ил.

б) дополнительная литература:

1. Что такое Metasploit? Руководство для начинающих [Электронный ресурс]: //URL: https://habr.com/ru/company/varonis/blog/528578/ (дата обращения: 22.08.2021).

2. Фреймворк Metasploit, домашняя страница [Электронный ресурс]: //URL: https://www.metasploit.com/ (дата обращения: 22.08.2021).

3. GitHub проекта AFL++. [Электронный ресурс]: // URL: https://github.com/AFLplusplus/AFLplusplus (дата обращения: 22.08.2021).

4. GitHub проекта AFL-cov [Электронный ресурс]: // URL: https://github.com/mrash/afl-cov (дата обращения: 22.08.2021).

5. Санитайзеры Google. [Электронный ресурс]: // URL: https://github.com/google/sanitizers (дата обращения: 22.08.2021).

6. Jason Andress, Ryan Linn. Coding for Penetration Testers: Building Better Tools 2nd Edition

7. Nmap® Cookbook. The fat-free guide to network scanning

в) программное обеспечение и Интернет-ресурсы

1. Программное обеспечение Kali Linux. [Электронный ресурс]: //URL: https://www.kali.org/ (дата обращения: 22.08.2021).
2. Интернет ресурс База данных уязвимостей ФСТЭК России. [Электронный ресурс]: //URL: https://bdu.fstec.ru/ (дата обращения: 22.08.2021).
3. Интернет ресурс GitHub Института системного программирования российской академии наук им. В.П. Иванникова. [Электронный ресурс]: // URL: https://github.com/ispras/ (дата обращения: 22.08.2021).
4. Интернет ресурс Common Vulnerabilities and Exposures. [Электронный ресурс]: // URL: http://cve.mitre.org/ (дата обращения: 22.08.2021).
5. Интернет ресурс Common Weakness Enumeration. [Электронный ресурс]: // URL: https://cwe.mitre.org/ (дата обращения: 22.08.2021).

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Материально-техническое обеспечение включает в себя специально оборудованные кабинеты и аудитории: компьютерные классы, аудитории, оборудование мультимедийными средствами обучения.

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

При чтении лекционного материала используется электронное сопровождение курса: справочно-иллюстративный материал воспроизводится и озвучивается в аудитории с использованием проектора и переносного компьютера в реальном времени. Электронный материал доступен студентам для использования и самостоятельного изучения на сайте кафедры по адресу http://dozen.mephi.ru.

На сайте кафедры также находится методический и справочный материал, необходимый для проведения лабораторного практикума по курсу.

Лабораторный практикум проводится по расписанию в дисплейном классе одновременно для группы студентов, работающих в интерактивном режиме. Допустимо выполнение лабораторных работ в составе локальной сети кафедры или в удаленном режиме, используя Интернет.

Программа составлена в соответствии с требованиями ОС НИЯУ МИФИ по направлению подготовки (специальности): 09.04.02 «Информационные системы и технологии»»

Автор(ы)_____

Рецензент(ы)_____

Программа одобрена на заседании_____

_____