Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский ядерный университет «МИФИ»

ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ

КАФЕДРА КРИПТОЛОГИИ И ДИСКРЕТНОЙ МАТЕМАТИКИ

ОДОБРЕНО УМС ИИКС

Протокол № УМС-575/01-1

от 30.08.2021 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДАННЫХ

Направление подготовки (специальность) [1] 10.04.01 Информационная безопасность

Семестр	**Трудоемкость, кред.**	**Общий объем курса, час.**	**Лекции, час.**	**Практич. занятия, час.**	**Лаборат. работы, час.**	**В форме практической подготовки/ В**	**СРС, час.**	**КСР, час.**	**Форма(ы) контроля, экз./зач./КР/КП**
2	2	72	30	0	15		27	0	З
3	3	108	32	0	16		8-24	0	Э
Итого	5	180	62	0	31	0	35-51	0	

Москва, 2020

АННОТАЦИЯ

В курсе изучается внутренняя архитектура ОС Windows, в частности, основные компоненты ОС, их взаимодействия, а также работа и структура исполняемых файлов (PE-формат), используемых в ОС. При изучении исполняемых файлов внимание уделяется методам и средствам статического (использование дизассемблеров, декомпиляторов) и динамического анализа (использование дебаггеров, мониторов системных событий, песочниц). Помимо этого, будут рассмотрены механизмы противодействия анализу. Для статического – запаковка исполняемого кода, обфусцирующие и запутывающие преобразования кода, антидизассемблирование. Для динамического – приёмы антиотладки, антивиртуализации. Так же в курсе рассматриваются основы вирусной аналитики с методикой создания собственной аналитической программной лабораторией.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Цель дисциплины – изучение принципов и методов, используемых при защите программного обеспечения, а также методов и средств для обратной разработки программного обеспечения на примере ОС Windows.

В курсе рассматриваются следующие темы:

- внутренняя архитектура ОС Windows,
- основы обратной разработки программного обеспечения,
- построение исследовательской программной лаборатории для исследований,
- методы и средства статического анализа программного обеспечения,
- методы и средства противодействия статическому анализу программного обеспечения,
- методы и средства динамического анализа программного обеспечения,
- методы и средства противодействия динамическому анализу программного обеспечения,
- основы вирусной аналитики.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Полученные в результате освоения учебной дисциплины знания, умения, навыки используются в процессе дипломного проектирования.

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
ОПК-5 [1] – Способен проводить научные исследования, включая экспериментальные, обрабатывать	З-ОПК-5 [1] – Знать: теоретические и эмпирические методы научных исследований, порядок проведения научных исследований

результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи	У-ОПК-5 [1] – Уметь: применять методы научных исследований в научной деятельности, обобщать полученные экспериментальные данные, анализировать и делать выводы В-ОПК-5 [1] – Владеть: теоретическими и эмпирическими методами научного исследования при выполнении научно-исследовательских работ, методикой оформления отчетов по научно-исследовательским работам, статей и тезисов докладов

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

Задача профессиональной деятельности (ЗПД)	**Объект или область знания**	**Код и наименование профессиональной компетенции; Основание (профессиональный стандарт-ПС, анализ опыта)**	**Код и наименование индикатора достижения профессиональной компетенции**
проектный			
разработка проектных решений по обеспечению безопасности данных с применением криптографических методов	информационные ресурсы	ПК-1 [1] - Способен принимать участие в разработке систем обеспечения ИБ или информационно-аналитических систем безопасности *Основание:* Профессиональный стандарт: 06.032	З-ПК-1[1] - Знать: модели угроз нсд к сетям электросвязи; методики оценки уязвимостей сетей электросвязи с точки зрения возможности нсд к ним; нормативные правовые акты в области связи, информатизации и защиты информации; виды политик безопасности компьютерных систем и сетей; возможности используемых и планируемых к использованию средств защиты информации; особенности защиты информации в автоматизированных системах управления технологическими процессами; критерии оценки эффективности и надежности средств защиты информации программного обеспечения

			автоматизированных систем; основные характеристики технических средств защиты информации от утечек по техническим каналам; нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации; технические каналы утечки информации. ; У-ПК-1[1] - Уметь: выявлять и оценивать угрозы нсд к сетям электросвязи; анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия; классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; выбирать меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы; проводить анализ угроз безопасности информации на объекте информатизации; проводить предпроектное обследование объекта информатизации. ; В-ПК-1[1] - Владеть:

			основами проведения технических работ при аттестации сссэ с учетом требований по защите информации; определением угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети; основами разработки модели угроз безопасности информации и модели нарушителя в автоматизированных системах; основами предпроектного обследования объекта информатизации; основами разработки аналитического обоснования необходимости создания системы защиты информации на объекте информатизации (модели угроз безопасности информации).
разработка проектных решений по обеспечению безопасности данных с применением криптографических методов	информационные ресурсы	ПК-4.1 [1] - Способен разрабатывать проектные решения по обеспечению безопасности данных с применением криптографических методов *Основание:* Профессиональный стандарт: 06.032	З-ПК-4.1[1] - Знать: методы обеспечения безопасности данных с применением криптографических методов; У-ПК-4.1[1] - Уметь: разрабатывать проектные решения по обеспечению безопасности данных с применением криптографических методов; В-ПК-4.1[1] - Владеть: навыками разработки проектных решений по

			обеспечению безопасности данных с применением криптографических методов

4. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Разделы учебной дисциплины, их объем, сроки изучения и формы контроля:

№ п.п	Наименование раздела учебной дисциплины	Недели	Лекции/ Практ. (семинары)/ Лабораторные работы, час.	Обязат. текущий контроль (форма*, неделя)	Максимальный балл за раздел**	Аттестация раздела (форма*, неделя)	Индикаторы освоения компетенции
	2 Семестр						
1	Первый раздел	1-8			25	КИ-8	З-ПК-4.1, У-ПК-4.1, В-ПК-4.1, З-ОПК-5, У-ОПК-5, В-ОПК-5
2	Второй раздел	9-15			25	КИ-15	З-ПК-4.1, У-ПК-4.1, В-ПК-4.1, З-ОПК-5, У-ОПК-5, В-ОПК-5

	Итого за 2 Семестр		30/0/15		50		
	Контрольные мероприятия за 2 Семестр				50	З	З-ПК-4.1, У-ПК-4.1, В-ПК-4.1, З-ОПК-5, У-ОПК-5, В-ОПК-5
	3 Семестр						
1	Первый раздел	1-8			25	КИ-8	З-ОПК-5, У-ОПК-5, В-ОПК-5, З-ПК-4.1, У-ПК-4.1, В-ПК-4.1
2	Второй раздел	9-16			25	КИ-16	З-ОПК-5, У-ОПК-5, В-ОПК-5, З-ПК-4.1, У-ПК-4.1, В-ПК-

							4.1
	Итого за 3 Семестр		32/0/16		50		
	Контрольные мероприятия за 3 Семестр				50	Э	З-ОПК-5, У-ОПК-5, В-ОПК-5, З-ПК-4.1, У-ПК-4.1, В-ПК-4.1

* – сокращенное наименование формы контроля

** – сумма максимальных баллов должна быть равна 100 за семестр, включая зачет и (или) экзамен

Сокращение наименований форм текущего контроля и аттестации разделов:

Обозначение	**Полное наименование**
КИ	Контроль по итогам
З	Зачет
Э	Экзамен

КАЛЕНДАРНЫЙ ПЛАН

Недели	**Темы занятий / Содержание**	**Лек., час.**	**Пр./сем., час.**	**Лаб., час.**
	2 Семестр	30	0	15
1-8	**Первый раздел**	16		8
1 - 4	**Задачи и проблемы защиты программного обеспечения** Задачи защиты программного обеспечения. Требования к ним. Проблемы защиты программного обеспечения.	Всего аудиторных часов		
		8		4
		Онлайн		
5 - 8	**Регистры процессора и основы ассемблера** Регистры процессоров X86-X64: общего назначения, регистр флагов, регистры математического сопроцессора. Команды ассемблера: математические, логические, условные, адресные, работы со стеком. Стандартные шаблоны программирования в дизассеблированном виде. Работа со страницами памяти.	Всего аудиторных часов		
		8		4
		Онлайн		
9-15	**Второй раздел**	14		7
9 - 12	**Формат PE-файла**	Всего аудиторных часов		

	Структура PE-файла. DOS-заголовок. PE-заголовок. Секции файла. Каталоги данных (таблица импорта, таблица экспорта)	8		4
		Онлайн		
13 - 15	**Введение в вирусную аналитику** Определение вредоносного ПО. Классификация вредоносного ПО. Создание аналитической программной лаборатории. Принципы использования аналитической программной лаборатории. Виртуализация.	Всего аудиторных часов		
		6		3
		Онлайн		
	3 Семестр	32	0	16
1-8	**Первый раздел**	16		8
1 - 4	**Статический анализ и противодействие ему** Использование дизассемблеров, декомпиляторов (IDA Pro, dnSpy). Статический сбор артефактов об исследуемом ПО. (PEStudio) Запаковка программного обеспечения. Методы обфускации. Примеры антидизассемблирования.	Всего аудиторных часов		
		8		4
		Онлайн		
5 - 8	**Динамический анализ и противодействие ему** Использование дебаггеров (IDA Pro, OllyDbg). Мониторы системных событий и функций (Process Monitor, API Monitor). Перехват трафика (Wireshark, Fiddler). Песочницы. Антиотладочные трюки. Определение виртуализации.	Всего аудиторных часов		
		8		4
		Онлайн		
9-16	**Второй раздел**	16		8
9 - 16	**Архитектура ОС Windows** Архитектура Windows. Стандартные библиотеки. Приложения и службы. Подсистемы в Windows. Компоненты ядра. Основные структуры: процессы, потоки, сокеты, файлы, реестр.	Всего аудиторных часов		
		16		8
		Онлайн		

Сокращенные наименования онлайн опций:

Обозначение	**Полное наименование**
ЭК	Электронный курс
ПМ	Полнотекстовый материал
ПЛ	Полнотекстовые лекции
ВМ	Видео-материалы
АМ	Аудио-материалы
Прз	Презентации
Т	Тесты
ЭСМ	Электронные справочные материалы
ИС	Интерактивный сайт

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Основными образовательными технологиями в освоении дисциплин профессионального цикла являются традиционные технологии лекций и лабораторных работ. Интерактивные методики обеспечиваются решением индивидуальных задач студентами и коллективным обсуждением результатов и методов решения.

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

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

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

Компетенция	**Индикаторы освоения**	**Аттестационное мероприятие (КП 1)**	**Аттестационное мероприятие (КП 2)**
ОПК-5	З-ОПК-5	З, КИ-8, КИ-15	Э, КИ-8, КИ-16
	У-ОПК-5	З, КИ-8, КИ-15	Э, КИ-8, КИ-16
	В-ОПК-5	З, КИ-8, КИ-15	Э, КИ-8, КИ-16
ПК-4.1	З-ПК-4.1	З, КИ-8, КИ-15	Э, КИ-8, КИ-16
	У-ПК-4.1	З, КИ-8, КИ-15	Э, КИ-8, КИ-16
	В-ПК-4.1	З, КИ-8, КИ-15	Э, КИ-8, КИ-16

Шкалы оценки образовательных достижений

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:

Сумма баллов	Оценка по 4-ех балльной шкале	Оценка ECTS	Требования к уровню освоению учебной дисциплины
90-100	5 – *«отлично»*	A	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.
85-89	4 – «*хорошо*»	B	Оценка «хорошо» выставляется студенту, если он твёрдо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.
75-84		C	
70-74		D	
65-69	3 – «*удовлетворительно*»		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.
60-64		E	
Ниже 60	2 – «*неудовлетворительно*»	F	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.

Оценочные средства приведены в Приложении.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. 004 М 21 Глобальная культура кибербезопасности : , Москва: Горячая линия -Телеком, 2018

2. 004 М 21 Комментарии к Доктрине информационной безопасности Российской Федерации. : , Москва: Горячая линия -Телеком, 2018

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

Специальное программное обеспечение не требуется

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

https://online.mephi.ru/

http://library.mephi.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Специальное материально-техническое обеспечение не требуется

9. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ

приложены

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

приложены

Автор(ы):

Когос Константин Григорьевич, к.т.н.