

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 КИБЕРБЕЗОПАСНОСТИ

ОДОБРЕНО УМС ИИКС

Протокол № 8/1/2025

от 25.08.2025 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ЗАЩИТА ОТ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Направление подготовки
(специальность)

[1] 10.03.01 Информационная безопасность

Семестр	Трудоемкость, кред.	Общий объем курса, час.	Лекции, час.	Практич. занятия, час.	Лаборат. работы, час.	В форме практической подготовки, час.	СРС, час.	КСР, час.	Форма(ы) контроля, экз./зач./КР/КП
5	2	72	48	0	0		24	0	3
Итого	2	72	48	0	0	0	24	0	

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 дизассембляторов, 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

Курс основан на изучении таких дисциплин, как информатика, программирование, проектная практика. Навыки, полученные при изучении курса, используются студентами при дальнейшем обучении и подготовки выпускной квалификационной работы.

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
ОПК-1.3 [1] – Способен обеспечивать защиту информации при работе с базами данных, при	З-ОПК-1.3 [1] – знать методы защиты информации при работе с базами данных, при передаче информации по компьютерным сетям

передаче по компьютерным сетям	У-ОПК-1.3 [1] – уметь применять методы защиты информации при работе с базами данных, при передаче информации по компьютерным сетям В-ОПК-1.3 [1] – владеть навыками практического применения методов защиты информации при работе с базами данных, при передаче информации по компьютерным сетям
ОПК-1.4 [1] – Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями	З-ОПК-1.4 [1] – знать нормативными и корпоративными требованиями по безопасности компьютерных систем и сетей У-ОПК-1.4 [1] – уметь применять нормативные и корпоративные требования по безопасности компьютерных систем и сетей В-ОПК-1.4 [1] – владеть методами оценки уровня безопасности компьютерных систем и сетей

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; Основание (профессиональный стандарт-ПС, анализ опыта)	Код и наименование индикатора достижения профессиональной компетенции
организационно-управленческий			
организация работы по эксплуатации системы защиты информации, защищенных программно-аппаратных комплексов и распределённых информационных систем	системы защиты информации, программно-аппаратные комплексы и распределённые информационные системы	ПК-4.1 [1] - способен организовать работу по эксплуатации системы защиты информации, защищенных программно-аппаратных комплексов и распределённых информационных систем <i>Основание:</i> Профессиональный стандарт: 06.032	З-ПК-4.1[1] - знать принципы эксплуатации системы защиты информации, защищенных программно-аппаратных комплексов и распределённых информационных систем; У-ПК-4.1[1] - уметь организовать работу по эксплуатации системы защиты информации, защищенных программно-аппаратных комплексов и распределённых информационных систем; В-ПК-4.1[1] - владеть

			навыками эксплуатации системы защиты информации, защищенных программно-аппаратных комплексов и распределенных информационных систем
организация работы по эксплуатации системы защиты информации, защищенных программно-аппаратных комплексов и распределенных информационных систем	системы защиты информации, программно-аппаратные комплексы и распределенные информационные системы	ПК-4 [1] - способен разрабатывать предложения по совершенствованию системы управления безопасностью информации в организации <i>Основание:</i> Профессиональный стандарт: 06.032	З-ПК-4[1] - знать методы построения системы управления безопасностью информации ; У-ПК-4[1] - уметь разрабатывать предложения по совершенствованию системы управления безопасностью информации в организации; В-ПК-4[1] - владеть принципами построения системы управления безопасностью информации

4. ВОСПИТАТЕЛЬНЫЙ ПОТЕНЦИАЛ ДИСЦИПЛИНЫ

Направления/цели воспитания	Задачи воспитания (код)
Профессиональное воспитание	Создание условий, обеспечивающих, формирование культуры информационной безопасности (B23)
Профессиональное воспитание	Создание условий, обеспечивающих, формирование профессионально значимых установок: не производить, не копировать и не использовать программные и технические средства, не приобретённые на законных основаниях; не нарушать признанные нормы авторского права; не нарушать тайны передачи сообщений, не практиковать вскрытие информационных систем и сетей передачи данных; соблюдать конфиденциальность доверенной информации (B40)

Защита от вредоносного программного обеспечения

5. 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
	<i>5 Семестр</i>						
1	Первый раздел	1-8	24/0/0		25	КИ-8	3-ОПК-1.3, У-ОПК-1.3, В-ОПК-1.3, 3-ОПК-1.4, У-ОПК-1.4, В-ОПК-1.4, 3-ПК-4.1, У-ПК-4.1, В-ПК-4.1, 3-ПК-4, У-ПК-4, В-ПК-4
2	Второй раздел	9-15	24/0/0		25	КИ-15	3-ОПК-1.3, У-ОПК-1.3, В-ОПК-1.3, 3-ОПК-1.4, У-ОПК-1.4, В-ОПК-1.4, 3-ПК-4.1, У-ПК-4.1, В-ПК-4.1, 3-ПК-4, У-ПК-4, В-ПК-4
	<i>Итого за 5 Семестр</i>		48/0/0		50		
	Контрольные мероприятия за 5 Семестр				50	3	3-ОПК-1.3, У-ОПК-1.3, В-ОПК-1.3, 3-ПК-4.1, У-ПК-4.1, В-ПК-4.1, 3-ПК-4, У-ПК-4, В-ПК-4

* – 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

КАЛЕНДАРНЫЙ ПЛАН

Недели	Темы занятий / Содержание	Лек., час.	Пр./сем., час.	Лаб., час.
	<i>5 Семестр</i>	48	0	0
1-8	Первый раздел	24	0	0
1 - 8	Раздел 1 Введение в защиту программного обеспечения	Всего аудиторных часов		
		24	0	0
		Онлайн		
		0	0	0
9-15	Второй раздел	24	0	0
9 - 16	Раздел 2 Обратная разработка программного обеспечения	Всего аудиторных часов		
		24	0	0
		Онлайн		
		0	0	0

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

6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Образовательные технологии сочетают в себе совокупность методов и средств для реализации определенного содержания обучения и воспитания в рамках дисциплины, включают решение дидактических и воспитательных задач, формируя основные понятия дисциплины, технологии проведения занятий, усвоения новых знаний, технологии повторения и контроля материала, самостоятельной работы.

7. 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)
ОПК-1.3	З-ОПК-1.3	З, КИ-8, КИ-15
	У-ОПК-1.3	З, КИ-8, КИ-15
	В-ОПК-1.3	З, КИ-8, КИ-15
ОПК-1.4	З-ОПК-1.4	КИ-8, КИ-15
	У-ОПК-1.4	КИ-8, КИ-15
	В-ОПК-1.4	КИ-8, КИ-15
ПК-4	З-ПК-4	З, КИ-8, КИ-15
	У-ПК-4	З, КИ-8, КИ-15
	В-ПК-4	З, КИ-8, КИ-15
ПК-4.1	З-ПК-4.1	З, КИ-8, КИ-15
	У-ПК-4.1	З, КИ-8, КИ-15
	В-ПК-4.1	З, КИ-8, КИ-15

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-х балльной шкале	Отметка о зачете	Оценка ECTS
90-100	5 – «отлично»	«зачтено»	A
85-89	4 – «хорошо»		B
75-84			C
70-74			D
65-69	3 – «удовлетворительно»		E
60-64			
ниже 60	2 – «неудовлетворительно»	«не зачтено»	F

Оценка «отлично» соответствует глубокому и прочному освоению материала программы обучающимся, который последовательно, четко и логически стройно излагает свои ответы, умеет тесно увязывать теорию с практикой, использует в ответах материалы монографической литературы.

Оценка «хорошо» соответствует твердым знаниям материала обучающимся, который грамотно и, по существу, излагает свои ответы, не допуская существенных неточностей.

Оценка «удовлетворительно» соответствует базовому уровню освоения материала обучающимся, при котором освоен основной материал, но не усвоены его детали, в ответах присутствуют неточности, недостаточно правильные формулировки, нарушения логической последовательности.

Отметка «зачтено» соответствует, как минимум, базовому уровню освоения материала программы, при котором обучающийся владеет необходимыми знаниями, умениями и навыками, умеет применять теоретические положения для решения типовых практических задач.

Оценку «неудовлетворительно» / отметку «не зачтено» получает обучающийся, который не знает значительной части материала программы, допускает в ответах существенные ошибки, не выполнил все обязательные задания, предусмотренные программой. Как правило, такие обучающиеся не могут продолжить обучение без дополнительных занятий.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

Специальное программное обеспечение не требуется

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

<https://online.mephi.ru/>

<http://library.mephi.ru/>

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Специальное материально-техническое обеспечение не требуется

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ

Студенты должны своевременно спланировать учебное время для поэтапного и системного изучения данной учебной дисциплины в соответствии с планом занятий, графиком контроля знаний.

Успешное освоение дисциплины требует от студентов активной работы во время занятий, выполнения всех домашних заданий, ознакомления с базовыми учебниками, основной и дополнительной литературой, а также предполагает творческое участие студента путем планомерной, повседневной работы.

Изучение дисциплины следует начинать с проработки учебной программы, особое внимание, уделяя целям и задачам, структуре и содержанию курса.

В процессе изучения учебной дисциплины необходимо обратить внимание на самоконтроль. Требуется регулярно отводить время для повторения пройденного материала, проверяя свои знания, умения и навыки по контрольным вопросам, а также для выполнения домашних заданий, которые выдаются после каждого занятия.

Систематическая индивидуальная работа, постоянная активность на занятиях, готовность ставить и обсуждать актуальные проблемы курса – залог успешной работы и положительной оценки.

11. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

Учебный курс строится на интегративной основе и включает в себя практические навыки, получаемые студентами в ходе практических и самостоятельных занятий.

Данная дисциплина выполняет функции практической подготовки студентов.

Содержание учебного курса, его объем и характер обуславливают необходимость оптимизации учебного процесса в плане отбора материала обучения и методики его организации, а также контроля текущей учебной работы. В связи с этим возрастает значимость и изменяется статус внеаудиторной (самостоятельной) работы, которая становится полноценным и обязательным видом учебно-познавательной деятельности студентов. При изучении курса самостоятельная работа включает:

самостоятельное ознакомление студентов с теоретическим материалом, представленным в отечественных и зарубежных научно-практических публикациях;

самостоятельное изучение тем учебной программы, достаточно хорошо обеспеченных литературой и сравнительно несложных для понимания;

Со стороны преподавателя должен быть установлен контакт со студентами, и они должны быть информированы о порядке прохождения курса, его особенностях, учебно-методическом обеспечении по данной дисциплине. Преподаватель дает методические рекомендации обучаемым по самостоятельному изучению проблем, характеризуя пути и средства достижения поставленных перед ними задач, высказывает советы и рекомендации по изучению учебной литературы, самостоятельной работе и работе на практических занятиях.

Автор(ы):

Матиев Джабраил Магомедович