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

ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ

КАФЕДРА КИБЕРНЕТИКИ

ОДОБРЕНО УМС ИИКС

Протокол № 8/1/2024

от 28.08.2024 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

РЕВЕРС-ИНЖИНИРИНГ

Направление подготовки (специальность) [1] 01.03.02 Прикладная математика и информатика

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
7	2	72	16	16	0		40	0	ЗО
Итого	2	72	16	16	0	16	40	0	

АННОТАЦИЯ

Данный учебный курс посвящен знакомству с основными видами бинарных уязвимостей, получению навыков статического и динамического анализа ПО, определению его скрытых возможностей и вредоносного функционала, а также изучению способов аллокации памяти и особенностей работы с каждым из них при написании ПО.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

1. Получение навыков статического и динамического анализа ПО, определения его скрытых возможностей и вредоносного функционала.
2. Знакомство с основными видами бинарных уязвимостей и способов защиты от них.
3. Изучение способов аллокации памяти и особенностей работы с каждым из них при написании ПО.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Изучение дисциплины базируется на следующих прослушанных ранее курсах: основы программирования, программирования на языке Python, объектно-ориентированное программирование, объекты и структуры данных. Основные положения учебного курса должны / могут быть использованы при изучении дисциплин: исследование программно-аппаратных уязвимостей, анализ защищенности программно-аппаратных комплексов, безопаность мобильных приложений и устройств и т.д. Также, полученные умения, навыки и знания необходимы для успешного выполнения научно–исследовательской работы.

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**

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**
производственно-технологический			
разработка и сопровождение программного обеспечения	информационные и программные системы	ПК-1.2 [1] - способен разрабатывать и применять прикладные программы при	З-ПК-1.2[1] - знать принципы построения и условия применения программ,

		решении задач в области киберфизических и информационных систем *Основание:* Профессиональный стандарт: 24.057, Анализ опыта: разработка математического и программного обеспечения киберфизических систем	используемых в задачах разработки и сопровождения киберфизических и информационных систем ; У-ПК-1.2[1] - уметь обоснованно выбирать алгоритмы и программные средства для решения задач проектирования и сопровождения киберфизических и информационных систем ; В-ПК-1.2[1] - владеть навыками использования прикладных программ при разработке и моделировании киберфизических и информационных систем
научно-исследовательский			
анализ и математическое моделирование физических процессов	системы ядерно-энергетического комплекса	ПК-2 [1] - Способен понимать, применять и совершенствовать современный математический аппарат *Основание:* Профессиональный стандарт: 24.078	З-ПК-2[1] - знать современный математический аппарат, используемый при описании, решении и анализе различных прикладных задач; У-ПК-2[1] - использовать современный математический аппарат для построения математических моделей и алгоритмов решения различных прикладных задач; В-ПК-2[1] - владеть навыками применения современного математического аппарата для построения математических моделей различных

			процессов, для обработки экспериментальных, статистических и теоретических данных, для разработки новых алгоритмов и методов исследования задач различных типов

4. ВОСПИТАТЕЛЬНЫЙ ПОТЕНЦИАЛ ДИСЦИПЛИНЫ

Направления/цели воспитания	**Задачи воспитания (код)**
Профессиональное воспитание	Создание условий, обеспечивающих, формирование ответственности за профессиональный выбор, профессиональное развитие и профессиональные решения (В18)
Профессиональное воспитание	Создание условий, обеспечивающих, формирование научного мировоззрения, культуры поиска нестандартных научно-технических/практических решений, критического отношения к исследованиям лженаучного толка (В19)
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 (В40)

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**
	7 Семестр						

1	Первый раздел	1-8	8/8/0		25	КИ-8	З-ПК-1.2, У-ПК-1.2, В-ПК-1.2, З-ПК-2, У-ПК-2, В-ПК-2
2	Второй раздел	9-16	8/8/0		25	КИ-16	З-ПК-1.2, У-ПК-1.2, В-ПК-1.2, З-ПК-2, У-ПК-2, В-ПК-2
	Итого за 7 Семестр		16/16/0		50		
	Контрольные мероприятия за 7 Семестр				50	ЗО	З-ПК-1.2, У-ПК-1.2, В-ПК-1.2, З-ПК-2, У-ПК-2, В-ПК-2

* – 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**
ЗО	Зачет с оценкой
КИ	Контроль по итогам
З	Зачет

КАЛЕНДАРНЫЙ ПЛАН

Недели	**Темы занятий / Содержание**	**Лек., час.**	**Пр./сем., час.**	**Лаб., час.**
	7 Семестр	16	16	0
1-8	**Первый раздел**	8	8	0
1 - 2	**1.1** Ревенс-инжиниринг .net framework-приложений, знакомство с IlSpy, Dis#, dnSpy, DotPeek	Всего аудиторных часов		
		2	2	0
		Онлайн		
		0	0	0
3 - 4	**1.2** Изучение и распаковка протекторов .net приложений	Всего аудиторных часов		
		2	2	0
		Онлайн		
		0	0	0
5 - 6	**1.3** Знакомство с нативным кодом, регистры, опкоды, ассемблер, структура памяти приложения. Знакомство с IDA Pro и hex-rays..	Всего аудиторных часов		
		2	2	0
		Онлайн		
		0	0	0
7 - 8	**1.4**	Всего аудиторных часов		

	Динамическая отладка приложений, знакомство с x64dbg, gdb и ollydbg	2	2	0
		Онлайн		
		0	0	0
9-16	**Второй раздел**	8	8	0
9 - 10	**2.1** Распаковка протекторов нативных приложений и драйверов	Всего аудиторных часов		
		2	2	0
		Онлайн		
		0	0	0
11 - 12	**2.2** Реверс-Инжиниринг java приложений и приложений ОС Android	Всего аудиторных часов		
		2	2	0
		Онлайн		
		0	0	0
13 - 14	**2.3** Бинарные уязвимости. Переполнение стека, кучи, форматная строка, use-after-free. Техники эксплуатации и защиты.	Всего аудиторных часов		
		2	2	0
		Онлайн		
		0	0	0
15 - 16	**2.4** Протекторы на основе виртуального кода. Создание дизассемблера виртуального кода. Реверс-инжиниринг прошивки микроконтроллера	Всего аудиторных часов		
		2	2	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

В ходе занятий рассматриваются практические задачи, делается акцент на прикладные исследования. Студенты получают опыт самостоятельного исследования исполняемых файлов, улучшают навыки дизассемблирования и декомпилирония, учатся систематизировать и представлять результаты исследований в виде отчетов, а также проводить анализ и изменения программного кода для повышения его безопасности.

При обсуждении тем практических занятий используются интерактивные формы обучения, в частности, используются презентации, обсуждаются последние научные работы, передовые технологии компиляции исходного кода и анализа скомпилированного кода, рассказывается о работе с научной литературой. Обязательным является самостоятельная работа студентов, выполнение индивидуальных заданий, работа с литературой.

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)**
ПК-1.2	З-ПК-1.2	ЗО, КИ-8, КИ-16
	У-ПК-1.2	ЗО, КИ-8, КИ-16
	В-ПК-1.2	ЗО, КИ-8, КИ-16
ПК-2	З-ПК-2	ЗО, КИ-8, КИ-16
	У-ПК-2	ЗО, КИ-8, КИ-16
	В-ПК-2	ЗО, 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:

<table>
<tr><th>Сумма баллов</th><th>Оценка по 4-х балльной шкале</th><th>Отметка о зачете</th><th>Оценка ECTS</th></tr>
<tr><td>90-100</td><td>5 – «отлично»</td><td rowspan="7">«Зачтено»</td><td>A</td></tr>
<tr><td>85-89</td><td rowspan="3">4 – «хорошо»</td><td>B</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></tr>
<tr><td>60-64</td><td>E</td></tr>
<tr><td>Ниже 60</td><td>2 – «неудовлетворительно»</td><td>«Не зачтено»</td><td>F</td></tr>
</table>

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:

1. Денис Юричев. Реверс-инжиниринг для начинающих (http://library.bagrintsev.me/unsorted/RE_for_beginners-ru.pdf)

2. Реверсинг малвари для начинающих (https://xakep.ru/2016/12/08/reversing-malware-tutorial-part1/#toc05.5)

3. Реверс-инжиниринг встраиваемых систем (https://dmkpress.com/catalog/electronics/circuit_design/978-5-93700-231/)

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

В курсе излагаются способы статического и динамического анализа ПО, выявления в нем основных видов бинарных уязвимостей, определению его скрытых возможностей и вредоносного функционала, а также изучению способов аллокации памяти и особенностей работы с каждым из них при написании ПО. Используя прослушанный на лекциях материал, студенты должны научиться решать поставленные перед ними задачи. Практика показала, что для наиболее эффективного усвоения студентами материала данной дисциплины необходимо использовать интерактивные формы проведения занятий с привлечением мультимедийных

технологий. В рамках занятий следует проводить активное обсуждение, проводить групповой поиск ответов на вопросы, возникающие у студентов при подготовке заданий и во время лекционных занятий. Основной упор на занятиях должен делаться на понимание излагаемого материала и умение его использовать при выполнении заданий.

На каждом занятии отмечается посещаемость студентов.

При изучении курса студентам рекомендуется внимательно ознакомиться с программой дисциплины, взять в библиотеке рекомендованную литературу.

Организация контроля успеваемости студентов проводится с использование фонда оценочных средств по данной дисциплине (ФОС). Фонд оценочных средств (ФОС) – является неотъемлемой частью учебно-методического комплекса учебной дисциплины и предназначен для контроля и оценки образовательных достижений обучающихся, освоивших программу данной дисциплины.

Рубежный контроль проводится на 8 и 16 неделе. В конце семестра студенты сдают по дисциплине зачет с оценкой.

Для допуска к зачету необходимо закрыть на положительную оценку все предложенные в рамках текущего контроля лабораторные работы и большое домашнее задание.

11. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

В курсе излагаются способы статического и динамического анализа ПО, выявления в нем основных видов бинарных уязвимостей, определению его скрытых возможностей и вредоносного функционала, а также изучению способов аллокации памяти и особенностей работы с каждым из них при написании ПО. Используя прослушанный на лекциях материал, студенты должны научиться решать поставленные перед ними задачи. Практика показала, что для наиболее эффективного усвоения студентами материала данной дисциплины необходимо использовать интерактивные формы проведения занятий с привлечением мультимедийных технологий. В рамках занятий следует проводить активное обсуждение, проводить групповой поиск ответов на вопросы, возникающие у студентов при подготовке заданий и во время лекционных занятий. Основной упор на занятиях должен делаться на понимание излагаемого материала и умение его использовать при выполнении заданий.

На каждом занятии отмечается посещаемость студентов. Рекомендуется не допускать до сдачи контрольных мероприятий студентов, регулярно пропускающих занятия.

На первом занятии необходимо ознакомить студентов с программой дисциплины, а также предложить литературу, которая потребуется для успешного освоения материала.

При проведении текущего контроля успеваемости по дисциплине «Реверс-инжиниринг» используются

- Большое домашние задание
- Практические работы

Рубежный контроль проводится на 8 и 16 неделе. В конце семестра студенты сдают по дисциплине зачет с оценкой.

Для допуска к зачету необходимо закрыть на положительную оценку все предложенные в рамках текущего контроля лабораторные работы и большое домашнее задание.

Автор(ы):

Алюшин Виктор Михайлович, к.ф.-м.н.

Колобашкина Любовь Викторовна