Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 10.12.2025 15:48:55
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение
высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
Факультет информационных технологий

УТВЕРЖДЕНО
Декан факультета
Информационных технологий
_____ / Д.Г. Демидов /
«16» 02 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Анализ и реверс инжиниринг программных средств»

Направление подготовки
10.03.01 «Информационная безопасность»

Профиль
«Безопасность компьютерных систем»

Квалификация
Бакалавр

Формы обучения
очная

Москва, 2023 г.

Разработчик(и):

Старший преподаватель, кафедра «Информационная безопасность»

 /А.А. Недогарок/

Согласовано:
Заведующий кафедрой «Информационная безопасность»

 /И.В. Калуцкий/

Руководитель образовательной программы,

 /А.Ю. Гневшев/

Содержание

1 Цели, задачи и планируемые результаты обучения по дисциплине 4
2 Место дисциплины в структуре образовательной программы 4
3 Структура и содержание дисциплины 5
3.1 Виды учебной работы и трудоемкость 5
3.2 Тематический план изучения дисциплины 5
4 Учебно-методическое и информационное обеспечение 6
4.1 Основная литература 6
4.2 Дополнительная литература 6
5 Материально-техническое обеспечение 7
6 Методические рекомендации 7
6.1 Методические рекомендации для преподавателя по организации обучения 7
6.2 Методические указания для обучающихся по освоению дисциплины 7
7 Фонд оценочных средств 7
7.1 Методы контроля и оценивания результатов обучения 7
7.2 Шкала и критерии оценивания результатов обучения 7
7.3 Оценочные средства 11
7.3.1 Список вопросов для экзамена 11

1 Цели, задачи и планируемые результаты обучения по дисциплине

К **основным целям** освоения дисциплины «Анализ и реверс инжиниринг программных средств» следует отнести получение системных знаний и навыков для практического применения анализа и реверс-инжиниринга программного обеспечения в кибербезопасности.

К **основным задачам** освоения дисциплины «Анализ и реверс инжиниринг программных средств» следует отнести:

- Изучение принципов работы прикладных программ на уровне команд языка ассемблера, их взаимодействие с центральным процессором, памятью, операционной системой.
- Получение навыков владения инструментами реверс-инжиниринга: декомпиляторами, дизассемблерами, отладчиками, эмуляторами и другими.
- Освоение методик анализа и реверс-инжиниринга программ для определения их структуры и алгоритмов работы.
- Получение навыков использования полученных знаний и умений при выявлении уязвимостей программного обеспечения, анализе зловредного кода, в форензике.
- Углубление знаний принципов и особенностей работы программного обеспечения, операционных систем и языков программирования, полученных ранее на других изученных курсах.

Обучение по дисциплине «Анализ и реверс инжиниринг программных средств» направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	**Индикаторы достижения компетенции**
ОПК-7. Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности	**знать:** • реверс инжиниринг программно-аппаратных решений; • разработка программного обеспечения; • исследование и анализ программного кода; • написание отчетной и технической документации о выполненных работах. **уметь:** • применять на практике знания, полученные в области реверс инжиниринга программного кода. **владеть:** • навыками исследования и анализа программного кода и написания отчётной, технической документации.

2 Место дисциплины в структуре образовательной программы

Дисциплина «Анализ и реверс инжиниринг программных средств» относится к числу профессиональных учебных дисциплин части формируемой участниками образовательных отношений (Б1.2) основной образовательной программы (Б1.2.04).

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: Языки программирования, Технологии и методы программирования.

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы, т.е. **144** академических часов (лабораторные занятия – 72 час, самостоятельная работа - 72 часов, форма контроля – экзамен) в 7 семестре.

Структура и содержание дисциплины «Анализ и реверс инжиниринг программных средств» по срокам и видам работы отражены в пунктах 3.1 и 3.2.

3.1 Виды учебной работы и трудоемкость (по формам обучения)

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
			Семестр	Неделя семестра
1	**Аудиторные занятия**	**72**	7	1-18
	В том числе:			
1.1	Лекции			
1.2	Семинарские/практические занятия			
1.3	Лабораторные занятия	72	7	1-18
2	**Самостоятельная работа**	**72**	7	1-18
3	**Промежуточная аттестация**		7	19-21
	Экзамен			
	Итого:	**144**		

3.2 Тематический план изучения дисциплины (по формам обучения)

3.2.1 Очная форма обучения

№ п/п	Разделы/темы дисциплины	Трудоемкость, час					
		Всего	Аудиторная работа				Самостоятельная работа
			Лекции	Семинарские/практические занятия	Лабораторные занятия	Практическая подготовка	
1	Введение. Терминология, историческая справка, области	10			5		5

	применения реверс-инжиниринга, нормативные акты.						
2	Обзор и сравнение инструментов реверс-инжиниринга ПО. Функции и назначение дизассемблеров, отладчиков, HEX-редакторов, декомпиляторов и других инструментов.	10			5		5
3	Форматы исполняемых файлов. Формат Microsoft Windows PE, ELF, Mach O.	12			6		6
4	Регистры и машинные/ассемблерные команды для действий с плавающей точкой/запятой. Арифметика цифровых устройств: знаковые и беззнаковые числа, обратный и дополнительный код, формат числа с фиксированной и плавающей запятой/точкой, стандарт IEEE-754. Расширения архитектуры x86/x64 для аппаратного ускорения математических операций.	12			6		6
5	Виртуальная память. Стековая память. Механика работы функций и процедур, соглашения о вызовах.	10			5		5
6	Реверс-инжиниринг и исследование конструкций высокоуровневых компилируемых языков после сборки исполняемого кода. Оптимизация и режимы работы компиляторов. Основы владения дизассемблером. Поиск и навигация в дизассемблированном коде.	10			5		5
7	Важнейшие аспекты устройства операционных систем в контексте анализа и реверс-инжиниринга программ с пользовательским уровнем привилегий. API операционных систем: WinAPI и POSIX. Системные сообщения и очереди сообщений.	10			5		5
8	Методика анализа и реверс-инжиниринга программного обеспечения.	10			5		5
9	Спортивные и соревновательные области применения реверс-инжиниринга. Решение программ-задач (crackme). Соревнования формата Capture The Flag (CTF).	10			5		5
10	Приёмы защиты от реверс-инжиниринга: защита от дизассемблирования, отладки, эмуляции. Анализ защищённого кода.	10			5		5

11	Детектирование и анализ зловредного кода, антивирусная аналитика.	10			5		5
12	Аспекты работы загрузчика и ядра операционных систем и специальных режимов работы ЦП, необходимые для анализа и реверс-инжиниринга загрузчика ОС, модулей ядра, драйверов и низкоуровневого ПО, работающего непосредственно с аппаратным обеспечением. Реальный и защищённый режимы работы ЦП. Прерывания. Уровни привилегий кода.	10			5		5
13	Типы связывания библиотек при сборке программ на компилируемых языках. Элементы композиционного анализа. Распознавание библиотечных функций при статическом подключении. Технология Fast Library Identification and Recognition Technology (FLIRT). Распознавание библиотечных функций по паттерну графа потока исполнения.	10			5		5
14	Инструментация кода. Низкоуровневые аспекты работы динамических анализаторов и отладчиков.	10			5		5
Итого		**144**			**72**		**72**

3.3 Лабораторные работы

Лабораторная работа №1. Разделы и заголовки исполняемого файла формата PE.

Лабораторная работа №2. Реверс-инжиниринг конструкций высокоуровневых языков программирования.

Лабораторная работа №3. Реверс-инжиниринг и решение программы-задачи «crackme».

Лабораторная работа №4. Реверс-инжиниринг кода математического выражения с плавающей точкой.

4 Учебно-методическое и информационное обеспечение

4.1 Основная литература

1. Абрамов, Е.С. Машинно-ориентированное программирование: учебное пособие / Е.С. Абрамов, И.Д. Сидоров ; Министерство образования и науки РФ, Южный федеральный университет, Инженерно-технологическая академия. – Таганрог : Издательство Южного федерального университета, 2016. – 88 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=492941 (дата обращения: 19.08.2019). – ISBN 978-5-9275-2065-7. – Текст : электронный.

2. Пильщиков, В.Н. Программирование на языке ассемблера IBM PC : учебное пособие / В.Н. Пильщиков. – Москва : Диалог-МИФИ, 2014. – 288 с. : ил. – Режим доступа: по подписке.

– URL: http://biblioclub.ru/index.php?page=book&id=447687 (дата обращения: 19.08.2019). – Библиогр. в кн. – ISBN 5-86404-051-7. – Текст : электронный.

4.2 Дополнительная литература

1. Флоренсов, А.Н. Системное программное обеспечение : учебное пособие / А.Н. Флоренсов ; Минобрнауки России, Омский государственный технический университет. – Омск : Издательство ОмГТУ, 2017. – 139 с. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=493301 (дата обращения: 19.08.2019). – Библиогр. в кн. – ISBN 978-5-8149-2441-4. – Текст : электронный.

4.3 Электронные образовательные ресурсы

Электронный образовательный ресурс на разработке.

5 Материально-техническое обеспечение

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор или экран) – 1 комплект, либо беспроводной или кабельный доступ в интернет для преподавателя и учащихся с пропускной способностью не менее 3 Мбит/с на каждого участника для демонстрации материалов с компьютера преподавателя на экран учащихся с помощью систем видеоконференцсвязи.

Для проведения лабораторных занятий необходимо наличие компьютерных классов оборудованных современной вычислительной техникой из расчета одно рабочее место на одного обучаемого.

Оборудование и аппаратура

Компьютер под управлением операционная система Microsoft Windows или Linux (Ubuntu), с установленной средой разработки с поддержкой разработки на C или C++, интерпретатором языка Python, дизассемблером, отладчиком, Hex-редактором и эмулятором.

6 Методические рекомендации

6.1 Методические указания для обучающихся по освоению дисциплины

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются лекции.

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, готовятся к экзамену, а также самостоятельно изучают отдельные темы учебной программы.

7 Фонд оценочных средств

7.1 Методы контроля и оценивания результатов обучения

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- экзамен.

7.2 Шкала и критерии оценивания результатов обучения

Оценивание производится по сумме набранных баллов за лабораторные работы и задание экзамена.

За выполнение обязательных лабораторных работ ЛР1-4 в срок и без замечаний учащийся может набрать до 50 баллов:

- до 8 баллов за ЛР1,
- до 12 за ЛР2,
- до 25 за ЛР3,
- до 5 за ЛР4.

При наличии замечаний и нарушении сроков оценка может быть снижена преподавателем.

Выполнение лабораторных работ включает оформление отчёта, оформленного по ГОСТ 7.32 - 2017 и его защиту на очном занятии в виде ответа на один случайный вопрос из списка вопросов, представленных для подготовки к каждой лабораторной работе. Отчёт по лабораторной работе считается принятым после его проверки преподавателем и отсутствия замечаний.

К выполнению экзаменационного задания допускаются учащиеся, выполнившие 4 обязательные лабораторные работы. Экзамен проводится в виде выполнения многоэтапного практического задания. За выполнение экзаменационного задания учащиеся могут получить до 50 баллов. Оценка выставляется по сумме набранных баллов согласно системе:

- <65 неудовлетворительно,
- 65...74 удовлетворительно,
- 75...84 хорошо,
- >= 85 отлично.

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине (модулю):

ОПК-7 Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
знать: • реверс инжиниринг программно-аппаратных решений; • разработк	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие следующих знаний:	Обучающийся демонстрирует неполное соответствие следующих знаний: • реверс инжиниринг программно-	Обучающийся демонстрирует частичное соответствие следующих знаний: • реверс	Обучающийся демонстрирует полное соответствие следующих знаний: • реверс

ОПК-7 Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
а программного обеспечения; • исследование и анализ программного кода; • написание отчетной и технической документации о выполненных работах.	• реверс инжиниринг программно-аппаратных решений; • разработка программного обеспечения; • исследование и анализ программного кода; • написание отчетной и технической документации о выполненных работах..	аппаратных решений; • разработка программного обеспечения; • исследование и анализ программного кода; • написание отчетной и технической документации о выполненных работах. Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	инжиниринг программно-аппаратных решений; • разработка программного обеспечения; • исследование и анализ программного кода; • написание отчетной и технической документации о выполненных работах. , но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	инжиниринг программно-аппаратных решений; • разработка программного обеспечения; • исследование и анализ программного кода; • написание отчетной и технической документации о выполненных работах. , свободно оперирует приобретенными знаниями.

ОПК-7 Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
уметь: применять на практике знания, полученные в области реверс инжиниринга программного кода.	Обучающийся не умеет или в недостаточной степени умеет применять на практике знания, полученные в области реверс инжиниринга программного кода.	Обучающийся демонстрирует неполное соответствие следующих умений: применять на практике знания, полученные в области реверс инжиниринга программного кода. Допускаются значительные ошибки, проявляется недостаточность умений.	Обучающийся демонстрирует частичное соответствие следующих умений: применять на практике знания, полученные в области реверс инжиниринга программного кода. Умения освоены, но допускаются незначительные ошибки, неточности.	Обучающийся демонстрирует полное соответствие следующих умений: применять на практике знания, полученные в области реверс инжиниринга программного кода. Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности.
владеть: навыками исследования и анализа программного кода и написания отчётной, технической документации.	Обучающийся не владеет или в недостаточной степени владеет навыками исследования и анализа программного кода и написания отчётной, технической документации.	Обучающийся владеет навыками исследования и анализа программного кода и написания отчётной, технической документации, но допускаются значительные ошибки,	Обучающийся частично владеет навыками исследования и анализа программного кода и написания отчётной, технической документации, навыки освоены, но допускаются незначительные	Обучающийся в полном объеме владеет навыками исследования и анализа программного кода и написания отчётной, технической документации, свободно применяет полученные навыки в ситуациях

ОПК-7 Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
		проявляется недостаточность владения	ошибки, неточности, затруднения.	повышенной сложности.

Шкалы оценивания результатов промежуточной аттестации и их описание:

Форма промежуточной аттестации: экзамен.

Промежуточная аттестация обучающихся в форме экзамена проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Шкала оценивания	**Описание**
Отлично	Выполнены все виды учебной работы, предусмотренные учебным планом без замечаний. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Хорошо	Выполнены все виды учебной работы, предусмотренные учебным планом без замечаний. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в

	таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.
Удовлетворительно	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.
Неудовлетворительно	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

7.3 Оценочные средства

7.3.1 Список вопросов для экзамена

1. Нормативные акты, регулирующие применение реверс-инжиниринга ПО.
2. Дизассемблеры. Функции, назначение, принципы работы, ограничения.
3. Отладчики. Функции, назначение, принципы работы, ограничения.
4. Нех-редакторы. Функции, назначение, принципы работы, ограничения.
5. Эмуляторы. Функции, назначение, принципы работы, ограничения. Отличие эмуляции, виртуализации и контейнеризации.
6. Формат исполняемых файлов PE.
7. Формат исполняемых файлов ELF.
8. Архитектура ЦП. Машинные и ассемблерные команды. Разновидности ассемблеров и языков ассемблера.
9. Регистры ЦП общего назначения, регистры адресации стека и команд. Регистр флагов.
10. Расширения архитектуры x86/x64 для аппаратного ускорения математических операций. Знаковые и беззнаковые числа, обратный и дополнительный код, формат числа с фиксированной и плавающей запятой/точкой. Регистры и машинные/ассемблерные команды для действий с плавающей точкой/запятой.
11. Виртуализация памяти.
12. Стековая память. Механика работы функций и процедур, соглашения о вызовах.
13. API операционных систем. Системные сообщения и очереди сообщений.

14. Базовая методика анализа и реверс-инжиниринга программного обеспечения.
15. Обфускация. Принципы работы, назначение, области применения, методы преодоления.
16. Полиморфизм кода. Принципы работы, назначение, области применения, методы преодоления.
17. Непрямые вызовы процедур. Принципы работы, назначение, области применения, методы преодоления.
18. Защита кода виртуализацией. Принципы работы, назначение, области применения, методы преодоления.
19. Упаковка. Принципы работы, назначение, области применения, методы преодоления.
20. Методы защиты от отладки. Принципы, ограничения, методы преодоления.
21. Реальный и защищённый режимы работы ЦП. Прерывания. Уровни привилегий кода.
22. Типы связывания библиотек при сборке программ на компилируемых языках. Преимущества, недостатки, подходы к композиционному анализу.