

**УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«УНИВЕРСИТЕТ УПРАВЛЕНИЯ «ТИСБИ»**

Кафедра информационных технологий

Утверждаю
Зав. кафедрой
О.В.Федорова
Протокол заседания
кафедры № 10
от 06.04.2026

Рабочая программа дисциплины

Наименование дисциплины	Реверсивная инженерия
Направление подготовки	09.03.01 Информатика и вычислительная техника
Направленность (профиль) образовательной программы	Инженерия информационных систем
Год набора	2025, 2026

Составители:

Декан факультета компьютерных и инженерных наук, профессор лаборатории программной инженерии Маццара М.

Старший преподаватель лаборатории языков программирования и компиляторов Потёмкин А.С.

АНО ВО «Университет Иннополис»

Казань

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Разделы рабочей программы:

1. Краткая характеристика дисциплины (модуля).
2. Перечень планируемых результатов обучения.
3. Место дисциплины (модуля) в структуре основной профессиональной образовательной программы высшего образования (ОПОП ВО).
4. Объем, структура и содержание дисциплины (модуля).
5. Учебно-методическое обеспечение.
6. Материально-техническое обеспечение.
7. Оценочные и методические материалы.
8. Дополнительные сведения.

Программа составлена в соответствии с требованиями ОПОП ВО Университета Иннополис по данному направлению подготовки.

Форма обучения	Семестр	Трудоемкость дисциплины в		Контактная работа		Контроль, час.	Самостоятельная работа, час.	Форма промежуточной аттестации (экз./диф. зач./зач.)
		зачетных единицах	академических часах	Лекции, час.	Семинарские (практические) занятия, час.			
очная	8	4	144	30	30	18	66	экзамен

1. КРАТКАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ (МОДУЛЯ)

Изучение дисциплины (модуля) «Reverse Engineering / Реверсивная инженерия» обеспечивает формирование и развитие компетенций обучающихся в области разработки программного обеспечения, решения проблем на этапе пост-разработки, их применение для решения различных прикладных задач в рамках профессиональной деятельности. В ходе освоения дисциплины обучающиеся рассматривают теорию работы с языками ассемблера и основные аспекты обратной разработки.

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Целью освоения дисциплины (модуля) является формирование знаний, умений и навыков в рамках профессиональной деятельности, позволяющих успешно работать в избранной отрасли, а также обладать компетенциями, способствующими социальной мобильности, устойчивости и конкурентоспособности обучающегося в условиях современных рыночных отношений. Задачами дисциплины являются овладение навыками чтения кода на языке ассемблера и написания программ на высокоуровневых и низкоуровневых языках программирования, методами применения сложных конструкций в программировании, инструментами для реализации обратного программирования.

Компетенции, формируемые в результате освоения дисциплины (модуля) при проведении учебных занятий в форме контактной работы обучающихся с педагогическими работниками Университета и в форме самостоятельной работы обучающихся:

№ п/п	Код компетенции	Наименование компетенции	Индикаторы компетенций	Методы и технологии обучения, способствующие формированию компетенции
1.	ПК-2	Способен выполнять работы по созданию (модификации) и сопровождению информационных систем	Знать: архитектуру, устройство и функционирование вычислительных и информационных систем; устройство и функционирование современных информационных систем; современные стандарты информационного взаимодействия систем; программные средства и платформы инфраструктуры информационных технологий организаций; современные подходы и стандарты автоматизации организации (например, CRM, MRP, ERP, ITIL, ITSM); методы выявления требований. Уметь: разрабатывать	Метод контрольных вопросов; Проектная технология; Информационно – коммуникационная технология; Групповая технология; Кейс-технология; Технология проблемного обучения

			архитектуру, дизайн и прототипы информационной системы; разрабатывать метрики (количественные показатели) работы информационной системы; настраивать и создавать компоненты анализа программного решения информационной системы; исправлять дефекты и несоответствия в архитектуре и дизайне информационной системы, подтверждать исправление дефектов и несоответствий в коде информационной системы и документации к ней; проверять (верифицировать) архитектуру информационной системы, выполнять параметрическую настройку информационной системы; разрабатывать технологии обмена данными; разрабатывать базы данных информационной системы; осуществлять оптимизацию информационной системы; разрабатывать пользовательскую документацию; оценивать временные и материальные затраты на разработку информационной системы при заданных ресурсах. Владеть: методами оптимизации работы информационной системы и её компонентов; приемами интеграции информационной системы с техническим обеспечением заказчика.	
2.	ПК-3	Способен обеспечивать качество программного кода и программных продуктов	Знать: теорию автоматического и ручного тестирования; актуальные инструменты для проведения ручного и автоматического функционального и нагрузочного тестирования. Уметь: внедрять инструменты и системы статического анализа кода; использовать техники тест-дизайна; автоматизировать тестирование. Владеть: навыками проверки среды сборки и среды исполнения; составления тест-планов и тест-кейсов; прогнозирования сбоев и нахождения ошибок в продуктах;	Метод контрольных вопросов; Проектная технология; Информационно – коммуникационная технология; Групповая технология; Кейс-технология; Технология проблемного обучения

			составления технического задания на устранение найденных после тестирования недочётов; тестирования результатов прототипирования; контроля качества разработки программных решений для информационной системы; настройки и создания компонентов для анализа качества программного решения; оценки времени и ресурсов на тестирование компонентов информационной системы.	
--	--	--	--	--

Знания: сформированы систематические знания методов разработки программного обеспечения; методик проведения обратной разработки; способов установки приложений; языка ассемблера; языков программирования; современных и перспективных средств разработки программных продуктов, технических средств; методологии разработки программного обеспечения и технологии программирования.

Умения: сформированы умения исследовать устройства и приложения; исследовать программное обеспечение приложения; проводить обратную разработку приложения; читать код на языке ассемблера; определять наиболее значимые критерии качества программного продукта; выбирать средства реализации требований к программному обеспечению; применять методы и средства проектирования программного обеспечения.

Навыки (владения): сформировано владение навыками разработки программного обеспечения; владения машинным языком и основными языками программирования; владение методами обратной разработки приложений; владение методами анализа и тестирования требований, техниками тестирования; методами планирования проектных работ; методами и средствами проектирования программного обеспечения.

3. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВЫСШЕГО ОБРАЗОВАНИЯ (ОПОП ВО)

Данная учебная дисциплина (модуль) включена в «Блок 1. Дисциплины (модули)» образовательной программы по направлению подготовки 09.03.01 Информатика и вычислительная техника, направленность (профиль) образовательной программы «Инженерия информационных систем» и относится к части, формируемой участниками образовательных отношений, обеспечивает формирование профессиональных компетенций. Дисциплина (модуль) «Reverse Engineering / Реверсивная инженерия» позволяет обучающимся получить знания, умения и навыки для успешной профессиональной деятельности в области программного обеспечения компьютерных вычислительных систем и сетей,

автоматизированных систем обработки информации и управления. Дисциплина осваивается студентами при обучении в очной форме на 3 курсе в 8 семестре.

4. ОБЪЕМ, СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Объем дисциплины (модуля) составляет:

4 зачетные единицы, 144 академических часа, объем контактной работы — 60 академических часов.

Структура дисциплины (модуля):

№ раздела	Наименование раздела дисциплины (модуля)	Трудоемкость, академические часы			
		Очная форма			
		Контактная работа		Контроль, час.	Самостоятельная работа, час.
		Лекции, час.	Семинарские (практические) занятия, час.		
1.	Базовые понятия	7	7	0	16
2.	Работа с кодом	7	7	0	16
3.	Специфичное для ОС	8	8	0	17
4.	Разбор примеров из практики с использованием готовых инструментов	8	8	0	17
	Промежуточная аттестация - экзамен			18	
ИТОГО:		30	30	18	66

Содержание дисциплины (модуля):

№ раздела	Наименование раздела дисциплины (модуля)	Содержание дисциплины (модуля) по темам	Формируемые компетенции
1.	Базовые понятия	Образцы кода. Целочисленные типы данных. Логические операторы. Работа с битами. Более сложные примеры.	ПК-2; ПК-3
2.	Работа с кодом	Идентификация исполняемых файлов. Связь с внешним миром. Поиск нужных инструкций. Определение ISA.	
3.	Специфичное для ОС	Способы передачи аргументов при вызове функции. Системные вызовы. Linux Windows	
4.	Разбор примеров из практики с использованием готовых инструментов	Инструменты. Разбор примеров с открытым форматом файлов. Разбор примеров с закрытым форматом файлов.	

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Университет Иннополис обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства.

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронно-библиотечной системе (электронной библиотеке) и к электронной информационно-образовательной среде Университета (<https://my.university.innopolis.ru>). Электронно-библиотечная система и электронная информационно-образовательная среда обеспечивают возможность доступа, обучающегося из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети «Интернет» (далее — сеть «Интернет»), как на территории Университета, так и вне его.

Также обучающимся обеспечен доступ (удаленный доступ) к современным профессиональным базам данных и информационным справочным системам.

Перечень учебно-методического обеспечения дисциплины (модуля):

1. Непейвода, Н. Н. Стили и методы программирования: учебное пособие / Н. Н. Непейвода. — 4-е изд. — Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2025. — 295 с. — Режим доступа: <https://www.iprbookshop.ru/146400.html> — ЭБС «IPRbooks».

Дополнительная литература:

1. Сеницын, С. В. Основы разработки программного обеспечения на примере языка С : учебник / С. В. Сеницын, О. И. Хлыткин. — 4-е изд. — Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2025. — 211 с. — Режим доступа: <https://www.iprbookshop.ru/146374.html> — ЭБС «IPRbooks».
2. Tanenbaum, A. S. Distributed Operating Systems. — Publishing House: Pearson, 1994. — 648 p. — Режим доступа: https://portal.university.innopolis.ru/reading_hall/detail.php?ID=84988 — Электронный каталог научно-технической библиотеки АНО ВО «Университет Иннополис».

Дистанционная поддержка дисциплины (модуля)

Для дистанционной поддержки дисциплины используется система управления образовательным контентом Moodle, развернутая на портале АНО ВО «Университет Иннополис». Во время обучения все студенты получают индивидуальные пароли для входа в систему, в которой размещаются: программа курса, контрольные вопросы, задания, темы лекций с презентационными материалами и т. д.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

1. Университет располагает материально-технической базой, соответствующей действующим противопожарным правилам и нормам и обеспечивающей проведение всех видов дисциплинарной и междисциплинарной подготовки, практической и научно-исследовательской работ обучающихся, предусмотренных учебным планом.

2. Помещения, которые представляют собой учебные аудитории для проведения занятий лекционного типа, занятий семинарского (практического) типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы и помещения для хранения и профилактического обслуживания учебного оборудования. Помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Изучение дисциплины обеспечивается в учебных аудиториях, оснащенных:

- столами и стульями;
- компьютерной техникой;
- специализированным оборудованием, включая демонстрационное оборудование.

Перечень материально-технического оснащения учебных аудиторий конкретизируется приказом директора или уполномоченного им лица ежегодно и размещается на официальном сайте Университета в информационно-коммуникационной сети «Интернет» в подразделе «Материально-техническое обеспечение и оснащённость образовательного процесса. Доступная среда» раздела «Сведения об образовательной организации» по ссылке: <https://innopolis.university/sveden/objects>.

3. Для проведения занятий лекционного и семинарского (практического) типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации, соответствующие программе дисциплины (модуля).

4. Лаборатории Университета, в том числе Кибер-физическая лаборатория информационной безопасности «Иннокиберполигон» (<https://engineerschool.innopolis.university/innocyberpolygon>), Цифровая лаборатория искусственного интеллекта «InnoDataHub» (<https://engineerschool.innopolis.university/innodatahub>), Цифровая образовательная песочница для разработки передовых систем «DevOps Playground» (<https://engineerschool.innopolis.university/devops>), оснащены лабораторным и специализированным оборудованием. Перечень материально-технического оснащения и программного обеспечения лабораторий размещается на официальном сайте Университета по ссылке: <https://innopolis.university/sveden/objects>.

5. Помещения для самостоятельной работы обучающихся, в том числе приспособленные для использования инвалидами и лицами с ограниченными

возможностями здоровья, оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к в электронную информационно-образовательную среду Университета.

6. Обучающимся предоставляется доступ (в том числе удаленный) к ресурсам информационно-телекоммуникационной сети «Интернет», электронным ресурсам (в том числе электронным библиотечным системам, современным профессиональным базам данных и информационным справочным системам):

№	Ссылка на информационный ресурс	Наименование разработки в электронной форме	Доступность
Электронно-библиотечные системы:			
1.	http://www.iprbookshop.ru	Русскоязычная ЭБС на платформе «IPR Smart». Учебники и учебные пособия для университетов издательства «IPRbooks». Учебники и учебные пособия для лиц с ОВЗ	Индивидуальный неограниченный доступ
2.	http://e.lanbook.com	Русскоязычная ЭБС на платформе «Лань». Учебники и учебные пособия для университетов издательства «Лань». Учебники и учебные пособия для лиц с ОВЗ	Индивидуальный неограниченный доступ
Профессиональные базы данных:			
3.	http://search.ebscohost.com	Платформа EBSCOHost. Доступ к англоязычным полнотекстовым книгам	Индивидуальный неограниченный доступ
4.	https://portal.university.innopolis.ru/reading_hall	Электронный каталог научно-технической библиотеки АНО ВО «Университет Иннополис»	Для студентов, зарегистрированных в системе
5.	https://habr.com	База данных для IT-специалистов	Доступ свободный
6.	https://www.sciencedirect.com	База данных ScienceDirect	Доступ свободный
7.	https://elibrary.ru	Научная электронная библиотека	Доступ свободный
8.	https://link.springer.com	Полнотекстовая англоязычная БД Springer	Доступ из локальной сети УИ. Для удаленного доступа требуется регистрация из локальной сети УИ
9.	https://ar.cnki.net	База Данных Academic Reference. База данных полнотекстовых англоязычных ресурсов по всем академическим дисциплинам, опубликованных в Китае	Доступ из локальной сети УИ
10.	https://www.ams.org/journals	База данных англоязычных полнотекстовых журналов AMS Journals (2017–2022 гг.)	Доступ из локальной сети УИ
11.	https://www.dl.begellhouse.com/collections/6764f0021c05bd10.html	База данных англоязычных полнотекстовых журналов Begell	Доступ из локальной сети УИ
12.	https://saemobilus.sae.org/	База данных англоязычных полнотекстовых журналов SAE International SAE eJournals eBooks	Доступ из локальной сети УИ
13.	https://www.worldscientific.com	База данных англоязычных полнотекстовых журналов WorldScientific 2001–2022 гг.	Доступ из локальной сети УИ
14.	https://www.scitation.org/ebooks	AIPP E-Book Collection I + Collection II. Англоязычная База данных полнотекстовых электронных книг.	Доступ из локальной сети УИ
15.	https://ufn.ru/	Автономная некоммерческая организация Редакция журнала "Успехи физических наук". Электронный журнал на русском языке.	Доступ из локальной сети УИ

16.	https://sk.sagepub.com/books/discipline	SAGE Publications Ltd eBook Collections. Англоязычная База данных полнотекстовых электронных книг	Доступ из локальной сети УИ
17.	https://onlinelibrary.wiley.com/	The Wiley Journals Database Англоязычная База данных полнотекстовых электронных журналов	Доступ из локальной сети УИ
18.	https://www.mathnet.ru/	Полнотекстовая коллекция русскоязычных электронных математических журналов	Доступ из локальной сети УИ
19.	https://quantum-electron.lebedev.ru/arhiv/	Электронная версия журнала «Квантовая электроника»	Доступ из локальной сети УИ
20.	http://journals.rcsi.science/	Полнотекстовая коллекция журналов Российской академии наук включает 140 наименований журналов, охватывающих различные научные специальности.	Доступ из локальной сети УИ
21.	https://www.orbit.com/	База данных патентного поиска, объединяющая информацию о более чем 122 миллионах патентных публикаций, полученную из 120 международных патентных ведомств, включая РосПатент, Всемирную организацию интеллектуальной собственности (ВОИС), Европейскую патентную организацию.	Доступ из локальной сети УИ
Информационные справочные системы:			
22.	https://minobrnauki.gov.ru/	Официальный сайт Министерства науки и высшего образования Российской Федерации	Доступ свободный
23.	https://www.edu.ru/	Федеральный портал «Российское образование»	Доступ свободный
24.	http://window.edu.ru/	Информационная система "Единое окно доступа к образовательным ресурсам"	Доступ свободный
25.	http://school-collection.edu.ru/	Единая коллекция цифровых образовательных ресурсов	Доступ свободный
26.	http://fcior.edu.ru/	Федеральный центр информационно-образовательных ресурсов	Доступ свободный

7. Университет Иннополис обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, в который входят:

Наименование ПО	Производство	Лицензионное / свободно распространяемое
Операционные системы:		
Microsoft Imagine (Windows Client, Server)	зарубежное	лицензионное
Браузеры:		
Яндекс.Браузер	отечественное	свободно распространяемое
Google Chrome	зарубежное	свободно распространяемое
Офисные приложения:		
Microsoft Imagine (Visio, OneNote)	зарубежное	лицензионное
TeXstudio	зарубежное	свободно распространяемое
Adobe Acrobat Reader	зарубежное	свободно распространяемое
Программное обеспечение для планирования и учета времени:		
Toggle app	зарубежное	свободно распространяемое
Системы управления проектами:		
Microsoft Imagine (Project)	зарубежное	лицензионное
Системы управления базами данных:		
Microsoft Imagine (SQL Server)	зарубежное	лицензионное

Системы резервного копирования (backup):		
Acronis Backup Advanced for HyperV	зарубежное	лицензионное
Справочно-правовые системы:		
КонсультантПлюс: справочно-правовая система	отечественное	лицензионное
Системы управления обучением:		
Система LMS Moodle	зарубежное	свободно распространяемое
Средства антивирусной защиты:		
Kaspersky Endpoint Security для бизнеса Стандартный Russian Edition	отечественное	лицензионное
Среды разработки:		
Visual Studio Code	зарубежное	свободно распространяемое
Bash (Unix shell)	зарубежное	свободно распространяемое
Anaconda	зарубежное	свободно распространяемое
Robotic Operating System	зарубежное	свободно распространяемое
CopelliaSim	зарубежное	свободно распространяемое
Google Colaboratory	зарубежное	свободно распространяемое
Пакеты программных средств и библиотек:		
AutoPsy	зарубежное	свободно распространяемое
Interactive Disassembler (IDA)	зарубежное	свободно распространяемое
Системы управления библиографической информацией:		
Zotero	зарубежное	свободно распространяемое
Сервисы и службы:		
Bind	зарубежное	свободно распространяемое
Docker	зарубежное	свободно распространяемое

7. МЕТОДИЧЕСКИЕ И ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Задания для семинарских (практических) занятий:

№ п/п	Наименование раздела дисциплины (модуля)	Перечень рассматриваемых тем (вопросов)
1.	Базовые понятия	Разработка отдельных частей кода программного продукта. 1. Написание простейших функций с изучением полученных результатов на машинном коде. - функция, которая ничего не делает - функция, возвращающее простое целочисленное значение - функция "Hello world" 2. Коррекция (патчинг) строки (win32 и win64) в исполняемом файле при помощи Hiew 3. Реализация концепции глобального указателя \$LC0: \000 это ноль в восьмеричной системе: .ascii "Hello, world!\012\000" main: <pre> lui \$28,%hi(__gnu_local_gp) addiu \$sp,\$sp,-32 addiu \$28,\$28,%lo(__gnu_local_gp) sw \$31,28(\$sp) lw \$25,%call16(puts)(\$28) lui \$4,%hi(\$LC0) jalr \$25 addiu \$4,\$4,%lo(\$LC0) ; branch delay slot lw \$31,28(\$sp) move \$2,\$0 </pre>

		<pre> j \$31 addiu \$sp,\$sp,32 ; 4. Вызов глобальных переменных и результаты в памяти #include <stdio.h> // x это глобальная переменная int x; int main() { printf ("Enter X:\n"); scanf ("%d", &x); printf ("You entered %d...\n", x); return 0; }; Результат на языке ассемблера: _DATA SEGMENT COMM _x:DWORD \$SG2456 DB 'Enter X:', 0aH, 00H \$SG2457 DB '%d', 00H \$SG2458 DB 'You entered %d...', 0aH, 00H _DATA ENDS PUBLIC _main EXTRN _scanf:PROC EXTRN _printf:PROC ; Function compile flags: /Odtp _TEXT SEGMENT _main PROC push ebp mov ebp, esp push OFFSET \$SG2456 call _printf add esp, 4 push OFFSET _x push OFFSET \$SG2457 call _scanf add esp, 8 mov eax, DWORD PTR _x push eax push OFFSET \$SG2458 call _printf add esp, 8 xor eax, eax pop ebp ret 0 _main ENDP _TEXT ENDS </pre>
2.	Работа с кодом	Разработка отдельных частей кода программного продукта 1. Работа с реестром. Расширение триального периода программного обеспечения 2. Поиск строк в бинарном файле 3. Написание кода на ассемблере <pre> MultiplyTest proc near ; CODE XREF: Get386Stepping xor cx, cx loc_620555: ; CODE XREF: MultiplyTest+E push cx call Multiply pop cx jb short locret_620563 loop loc_620555 </pre>

		<pre> clc locret_620563: ; CODE XREF: MultiplyTest+C retn MultiplyTest endp Multiply proc near ; CODE XREF: MultiplyTest+5 mov ecx, 81h mov eax, 417A000h mul ecx cmp edx, 2 stc jnz short locret_62057F cmp eax, 0FE7A000h stc jnz short locret_62057F clc locret_62057F: ; CODE XREF: Multiply+10 ; Multiply+18 retn Multiply endp </pre> 4. Поиск нужных инструкций и работа с полученными результатами, с целью разобрать полученный код, на примере Microsoft Excel и подсчета результатов формул, введенных пользователем. Например, операция деления. <pre>cat EXCEL.lst grep fddiv grep -v dbl_ > EXCEL.fdiv</pre>
3.	Специфичное для ОС	Разработка отдельных частей кода программного продукта 1. Реализация метода передачи аргументов, используя функцию thiscall <pre> #include <stdio.h> void f1(int a, int b, int c, int d, int e, int f, int g) { printf ("%d %d %d %d %d %d %d\n", a, b, c, d, e, f, g); }; int main() { f1(1,2,3,4,5,6,7); }; </pre> Результат на языке ассемблера <pre> \$SG2937 DB '%d %d %d %d %d %d %d', 0aH, 00H main PROC sub rsp, 72 mov DWORD PTR [rsp+48], 7 mov DWORD PTR [rsp+40], 6 mov DWORD PTR [rsp+32], 5 mov r9d, 4 mov r8d, 3 mov edx, 2 mov ecx, 1 call f1 xor eax, eax add rsp, 72 ret 0 main ENDP a\$ = 80 b\$ = 88 c\$ = 96 d\$ = 104 e\$ = 112 f\$ = 120 g\$ = 128 </pre>

		<pre> f1 PROC \$LN3: mov DWORD PTR [rsp+32], r9d mov DWORD PTR [rsp+24], r8d mov DWORD PTR [rsp+16], edx mov DWORD PTR [rsp+8], ecx sub rsp, 72 mov eax, DWORD PTR g\$[rsp] mov DWORD PTR [rsp+56], eax mov eax, DWORD PTR f\$[rsp] mov DWORD PTR [rsp+48], eax mov eax, DWORD PTR e\$[rsp] mov DWORD PTR [rsp+40], eax mov eax, DWORD PTR d\$[rsp] mov DWORD PTR [rsp+32], eax mov r9d, DWORD PTR c\$[rsp] mov r8d, DWORD PTR b\$[rsp] mov edx, DWORD PTR a\$[rsp] lea rcx, OFFSET FLAT:\$SG2937 call printf add rsp, 72 ret 0 f1 ENDP 2. Реализация генератора псевдослучайных чисел #include <stdint.h> #include <windows.h> #include <winnt.h> // from the Numerical Recipes book: #define RNG_a 1664525 #define RNG_c 1013904223 __declspec(thread) uint32_t rand_state; void my_srand (uint32_t init) { rand_state=init; } int my_rand () { rand_state=rand_state*RNG_a; rand_state=rand_state+RNG_c; return rand_state & 0x7fff; } int main() { my_srand(0x12345678); printf ("%d\n", my_rand()); }; 3. Обработка исключений с Windows SEH. Разработка программы с одним блоком try/except #include <stdio.h> #include <windows.h> #include <excpt.h> int main() { int* p = NULL; __try { printf("hello #1!\n"); *p = 13; // causes an access violation exception; printf("hello #2!\n"); </pre>
--	--	---

		<pre> } __except(GetExceptionCode()==EXCEPTION_ACCESS_VIOLATION ? EXCEPTION_EXECUTE_HANDLER : EXCEPTION_CONTINUE_SEARCH) { printf("access violation, can't recover\n"); } } </pre>
4.	Разбор примеров из практики с использованием готовых инструментов	Разработка отдельных частей кода программного продукта. - Шутка с task manager. Изменения в Task Manager, показывающие больше ядер в CPU, чем присутствует. - Поиск всех скрытых мин в игре сапёр, с использованием отладчика. <pre> #include <windows.h> #include <assert.h> #include <stdio.h> int main (int argc, char * argv[]) { int i, j; HANDLE h; DWORD PID, address, rd; 802 BYTE board[27][32]; if (argc!=3) { printf ("Usage: %s <PID> <address>\n", argv[0]); return 0; }; assert (argv[1]!=NULL); assert (argv[2]!=NULL); assert (sscanf (argv[1], "%d", &PID)==1); assert (sscanf (argv[2], "%x", &address)==1); h=OpenProcess (PROCESS_VM_OPERATION PROCESS_VM_READ PROCESS_VM_WRITE, FALSE, PID); if (h==NULL) { DWORD e=GetLastError(); printf ("OpenProcess error: %08X\n", e); return 0; }; if (ReadProcessMemory (h, (LPVOID)address, board, sizeof(board), &rd)!=TRUE) { printf ("ReadProcessMemory() failed\n"); return 0; }; for (i=1; i<26; i++) { if (board[i][0]==0x10 && board[i][1]==0x10) break; // end of board for (j=1; j<31; j++) { if (board[i][j]==0x10) break; // board border if (board[i][j]==0x8F) printf ("*"); else printf (" "); }; printf ("\n"); }; </pre>

		<pre> CloseHandle (h); }; 3. Изменение хода часов в обратную сторону. POINT rCircleTable[] = { { 0, -7999}, { 836, -7956}, { 1663, -7825}, { 2472, -7608}, { 3253, -7308}, ... { -4702, -6472}, { -3999, -6928}, { -3253, -7308}, { -2472, -7608}, { -1663, -7825}, 810 { -836, -7956}, }; void DrawHand(HDC, int pos, HPEN, int scale, int patMode, PCLOCKSTR np) { LPPOINT lppt; int radius; MoveTo(hDC, np->clockCenter.x, np->clockCenter.y); radius = MulDiv(np->clockRadius, scale, 100); lppt = rCircleTable + pos; SetROP2(hDC, patMode); SelectObject(hDC, hPen); LineTo(hDC, np->clockCenter.x + MulDiv(lppt->x, radius, 8000), np->clockCenter.y + MulDiv(lppt->y, radius, 8000)); } 4. Рисование множества Мандельброта using System; using System.Collections.Generic; using System.Linq; using System.Text; namespace Mnoj { class Program { static void Main(string[] args) { double realCoord, imagCoord; double realTemp, imagTemp, realTemp2, arg; int iterations; for (imagCoord = 1.2; imagCoord >= -1.2; imagCoord -= 0.05) { for (realCoord = -0.6; realCoord <= 1.77; realCoord += 0.03) { iterations = 0; realTemp = realCoord; imagTemp = imagCoord; </pre>
--	--	--

		<pre> arg = (realCoord * realCoord) + (imagCoord * imagCoord); while ((arg < 2*2) && (iterations < 40)) { realTemp2 = (realTemp * realTemp) - (imagTemp * imagTemp) - realCoord; imagTemp = (2 * realTemp * imagTemp) - imagCoord; realTemp = realTemp2; arg = (realTemp * realTemp) + (imagTemp * imagTemp); iterations += 1; } Console.WriteLine("{0,2:D} ", iterations); } Console.WriteLine("\n"); } Console.ReadKey(); } } } </pre>
--	--	--

Текущий контроль успеваемости обучающихся по дисциплине (модулю):

№ п/п	Наименование раздела дисциплины (модуля)	Форма текущего контроля	Материалы текущего контроля
1.	Базовые понятия	Проверка выполнения домашних заданий; Устный / письменный опрос; Защита проекта; Коллоквиум	Устный / письменный опрос: 1. Что такое язык ассемблера. 2. Что такое машинный код. 3. Представление чисел. 4. Различные системы счисления. Задания, в том числе, для групповых проектов: 1. Работа с thunk-функциями <pre>double Blas_Dot_Prod(const LaVectorDouble &dx, const LaVectorDouble &dy) { assert(dx.size()==dy.size()); integer n = dx.size(); integer incx = dx.inc(), incy = dy.inc(); return F77NAME(ddot)(&n, &dx(0), &incx, &dy(0), &incy); } </pre> 2. Реализация простых функций с использованием неоптимизирующего и оптимизирующего GCC
2.	Работа с кодом	Проверка выполнения домашних заданий; Устный / письменный опрос; Защита проекта; Коллоквиум	Задания, в том числе, для групповых проектов: 1. Идентифицируйте исполняемые файлы на C/C++ 2. Идентифицируйте исполняемые файлы на intel Fortran Устный / письменный опрос: 1. Перечислите часто используемые функции Windows API 2. Текстовые строки.
3.	Специфичное для ОС	Проверка выполнения домашних заданий; Устный /	Устный / письменный опрос: 1. Что выполняет функция cdecl? 2. Что выполняет функция stdcall? 3. Что выполняет функция fastcall? 4. Что выполняет функция thiscall?

		письменный опрос; Защита проекта; Коллоквиум	Задания, в том числе, для групповых проектов: 1. Модификация аргументов <pre>#include <stdio.h> void f(int a, int b) { a=a+b; printf ("%d\n", a); }; _a\$ = 8 _b\$ = 12 _f PROC push ebp mov ebp, esp mov eax, DWORD PTR _a\$[ebp] add eax, DWORD PTR _b\$[ebp] mov DWORD PTR _a\$[ebp], eax mov ecx, DWORD PTR _a\$[ebp] push ecx push OFFSET \$SG2938 ; '%d', 0aH call _printf add esp, 8 pop ebp ret 0 _f ENDP</pre>
4.	Разбор примеров из практики с использованием готовых инструментов	Проверка выполнения домашних заданий; Устный / письменный опрос; Защита проекта; Коллоквиум	Устный / письменный опрос: 1. Дизассемблеры 2. Отладчики 3. Декомпиляторы 4. Что такое проприетарный формат файлов Задания, в том числе, для групповых проектов: 1. Работа с зашифрованными данными в XML-файле 2. Работа с сетью. Функции проверки пароля в SAP

Контрольные вопросы для подготовки к промежуточной аттестации:

№ п/п	Наименование раздела дисциплины (модуля)	Наименование вопроса
1.	Базовые понятия	Пролог и эпилог функции. Рекурсия. Почему стек растет в обратную сторону. Передача параметров функции в ARM. Откуда берется мусор в стеке. Глобальные переменные. Как реализуется доступ к переданным аргументам. Возврат структуры. Указатели.
2.	Работа с кодом	UTF-8 Unicode UTF-16LE Константы. DHCP Циклы в бинарных файлах.

		Массивы в бинарных файлах. Случайные данные в дизассемблированном виде.
3.	Специфичное для ОС	Функции с переменным количеством аргументов. Указатель на аргумент функции. Принцип реализации. Thread Local Storage. Понятие "Базовый адрес". Критические секции. SEN3 и SEN4. Основные отличия. Что такое релок.
4.	Разбор примеров из практики с использованием готовых инструментов	Дизассемблер IDA Отладчик OllyDbg Отладчик GDB tracer Декомпилятор Hex-Rays Для чего может пригодиться калькулятор вовремя реверс инжиниринга Донглы

Вопросы/Задания к промежуточной аттестации в устной/письменной форме:

1. Пролог и эпилог функции.
2. Передача параметров функции в ARM.
3. Откуда берется мусор в стеке.
4. Указатели.
5. UTF-8. Unicode. UTF-16LE.
6. DHCP
7. Циклы в бинарных файлах. Массивы в бинарных файлах.
8. Случайные данные в дизассемблированном виде.
9. Функции с переменным количеством аргументов.
10. Указатель на аргумент функции. Принцип реализации.
11. Thread Local Storage.
12. Понятие «Базовый адрес».
13. Критические секции.
14. SEN3 и SEN4. Основные отличия.
15. Что такое релок.
16. Дизассемблер IDA
17. Отладчик OllyDbg
18. Отладчик GDB
19. tracer
20. Декомпилятор Hex-Rays

Критерии оценивания сформированности компетенций

Оценивание уровня учебных достижений, обучающихся по дисциплине (модулю), осуществляется в виде текущего контроля успеваемости и промежуточной аттестации.

В рамках внутренней системы оценки качества образовательной деятельности по программе обучающимся предоставляется возможность

оценивания условий, содержания, организации и качества образовательного процесса по данной дисциплине (модулю).

Промежуточная аттестация по дисциплине (модулю) осуществляется в форме экзамена, при этом проводится оценка компетенций, сформированных по дисциплине.

Система оценивания результатов обучения по дисциплине (модулю)

Знания, умения и навыки обучающихся при промежуточной аттестации определяются в следующей форме: «отлично» (А), «хорошо» (В), «удовлетворительно» (С), «неудовлетворительно» (D).

Критерии оценивания результатов обучения по дисциплине (модулю)

Результат обучения по дисциплине (модулю)	Общая характеристика результата обучения по дисциплине (модулю)
А «Отлично»	Обучающийся владеет знаниями предмета в полном объеме рабочей программы, достаточно глубоко осмысливает дисциплину; самостоятельно, в логической последовательности и исчерпывающе отвечает на все вопросы, подчеркивая при этом самое существенное, умеет анализировать, сравнивать, классифицировать, обобщать, конкретизировать и систематизировать изученный материал, выделять в нем главное: устанавливать причинно-следственные связи; четко формирует ответы, свободно читает результаты анализов и других исследований и решает ситуационные задачи повышенной сложности; хорошо знаком с основной литературой и методами исследования большого объема, необходимым для практической деятельности; увязывает теоретические аспекты предмета с задачами практического значения.
В «Хорошо»	Обучающийся владеет знаниями предмета практически в полном объеме рабочей программы; самостоятельно, в логической последовательности и исчерпывающе отвечает на все вопросы, подчеркивая при этом самое существенное, умеет анализировать, сравнивать, классифицировать, обобщать, конкретизировать и систематизировать изученный материал, выделять в нем главное: устанавливать причинно-следственные связи; четко формирует ответы, свободно читает результаты анализов и других исследований и решает ситуационные задачи повышенной сложности; хорошо знаком с основной литературой и методами исследования большого объема, необходимым для практической деятельности; увязывает теоретические аспекты предмета с задачами практического значения.
С «Удовлетворительно»	Обучающийся владеет основным объемом знаний по дисциплине; проявляет затруднения в самостоятельных ответах, оперирует неточными формулировками; в процессе ответов допускаются ошибки по существу вопросов. Обучающийся способен решать лишь наиболее легкие задачи, владеет только обязательным минимумом методов исследований.
D «Неудовлетворительно»	Обучающийся не освоил обязательного минимума знаний предмета, не способен ответить на вопросы даже при дополнительных наводящих вопросах преподавателя.

Методические указания для обучающихся по освоению дисциплины (модуля)

Вид учебных занятий/деятельности	Деятельность обучающегося
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения лекции, выводы, формулировки, обобщения; пометить важные мысли, выделять ключевые слова, термины. Обозначить вопросы, термины или другой материал, который вызывает трудности, пометить и попытаться найти

	ответ в рекомендуемой литературе. Если самостоятельно не удастся разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, во время семинарского (практического) занятия.
Практическое (семинарское) занятие	При подготовке к семинарскому (практическому) занятию необходимо проработать материалы лекций, основной и дополнительной литературы по заданной теме. На основании обработанной информации постараться сформировать собственное мнение по выносимой на обсуждение тематике. Обосновать его аргументами, сформировать список источников, подкрепляющих его. Во время семинарского (практического) занятия активно участвовать в обсуждении вопросов, высказывать аргументированную точку зрения на проблемные вопросы. Приводить примеры из источниковой базы и научной и/или исследовательской литературы.
Устный/письменный опрос	Отвечать, максимально полно, логично и структурировано, на поставленный вопрос. Основная цель – показать всю глубину знаний по конкретной теме или ее части.
Подготовка к промежуточной аттестации	При подготовке к промежуточной аттестации необходимо проработать вопросы по темам, которые рекомендуются для самостоятельной подготовки. При возникновении затруднений с ответами следует ориентироваться на конспекты лекций, семинаров, рекомендуемую литературу, материалы электронных и информационных справочных ресурсов, статей. Если тема вызывает затруднение, четко сформулировать проблемный вопрос и задать его преподавателю.
Практические (лабораторные) занятия	Практические занятия предназначены прежде всего для разбора отдельных сложных положений, тренировки аналитических навыков, а также для развития коммуникационных навыков. Поэтому на практических занятиях необходимо участвовать в тех формах обсуждения материала, которые предлагает преподаватель: отвечать на вопросы преподавателя, дополнять ответы других студентов, приводить примеры, задавать вопросы другим выступающим, обсуждать вопросы и выполнять задания в группах. Работа на практических занятиях подразумевает домашнюю подготовку и активную умственную работу на самом занятии. Работа на практических занятиях в форме устного опроса заключается прежде всего в тренировке навыков применять теоретические положения к самому разнообразному материалу. В ходе практических занятий студенты работают в группах для обсуждения предлагаемых вопросов.
Самостоятельная работа	Самостоятельная работа состоит из следующих частей: 1) чтение учебной, справочной, научной литературы; 2) повторение материала лекций; 3) составление планов устных выступлений; 4) подготовка видеопрезентации. При чтении учебной литературы нужно разграничивать для себя материал на отдельные проблемы, концепции, идеи. Учебную литературу можно найти в электронных библиотечных системах, на которые подписан АНО Университет Иннополис.
Дискуссия	Публичное обсуждение спорного вопроса, проблемы. Каждая сторона должна оппонировать мнение собеседника, аргументируя свою позицию.
Разработка отдельных частей кода	Разработать часть кода, исходя из поставленной задачи и рекомендаций преподавателя. При выполнении работы рекомендуется обращаться к материалам лекций и семинарских (практических) занятий. Если возникают затруднения, необходимо проконсультироваться с преподавателем.
Выполнение домашних заданий и групповых проектов	Для выполнения домашних заданий и групповых проектов необходимо получить формулировку задания от преподавателя и убедиться в понимании задания. При выполнении домашних заданий и групповых проектов необходимо проработать материалы лекций, основной и дополнительной литературы по заданной теме.

Для подготовки к занятиям рекомендуется использовать представленные источники в электронных форматах и дополнительную литературу.

8. ДОПОЛНИТЕЛЬНЫЕ СВЕДЕНИЯ

Данная программа и/или ее фрагменты не могут быть использованы другими образовательными организациями без соответствующего разрешения АНО ВО «Университет Иннополис».