Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Комсомольский-на-Амуре государственный университет»

УТВЕРЖДАЮ
Декан
факультета компьютерных технологий
(наименование факультета)
Я.Ю. Григорьев
(подпись, ФИО)
«04» 06 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Низкоуровневый анализ машинного кода

Направление подготовки	*10.05.03 "Информационная безопасность автоматизированных систем"*
Направленность (профиль) образовательной программы	*Анализ безопасности информационных систем*
Квалификация выпускника	*специалист по защите информации*
Год начала подготовки *(по учебному плану)*	*2021*
Форма обучения	*очная*
Технология обучения	*традиционная*

Курс	Семестр	Трудоемкость, з.е.
4	*8*	*3*

Вид промежуточной аттестации	Обеспечивающее подразделение
Зач_с_оц	*Кафедра ИБАС - Информационная безопасность автоматизированных систем*

Комсомольск-на-Амуре 2021

Разработчик рабочей программы:

доцент, К.Т.Н. _____ _____ _____

(должность, степень, ученое звание) (подпись) (ФИО)

СОГЛАСОВАНО:

Заведующий кафедрой

ИБАС _____ _____

(наименование кафедры) (подпись) (ФИО)

1 Общие положения

Рабочая программа дисциплины «Низкоуровневый анализ машинного кода» составлена в соответствии с требованиями федерального государственного образовательного стандарта, утвержденного приказом Министерства науки и высшего образования Российской Федерации № 1457 от 26.11.2020, и основной профессиональной образовательной программы подготовки «Анализ безопасности информационных систем» по специальности 10.05.03 "Информационная безопасность автоматизированных систем".

Практическая подготовка реализуется на основе:
Профессиональный стандарт утвержденного приказом Министерства труда и социальной защиты от 15 сентября 2016 года N 522н №843 "Специалист по защите информации в автоматизированных системах" зарегистрированного в Министерстве юстиции Российской Федерации 28 сентября 2016 года, регистрационный N 43857. Обобщенная трудовая функция: **С/03.6** Анализ уязвимостей внедряемой системы защиты информации.

Задачи дисциплины	• получение студентами знаний об основных синтаксических конструкциях языка ассемблер; • приобретение студентами навыков отладки программ на языке ассемблер; • получение опыта написания программ на языке ассемблер; • освоение теоретической и практической базы при работе с низкоуровневым кодом.
Основные разделы дисциплины	Основы организации ЭВМ, Низкоуровневый анализ машинного кода

2 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Процесс изучения дисциплины «Низкоуровневый анализ машинного кода» направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой (таблица 1):

Таблица 1 – Компетенции и индикаторы их достижения

Код и наименование компетенции	Индикаторы достижения	Планируемые результаты обучения по дисциплине
Общепрофессиональные		
ОПК-7.3. Способен проводить анализ защищенности и верификацию программного обеспечения информационных систем	**ОПК-7.3..1** Знает виды и порядок проведения анализа защищенности автоматизированных систем	Знает виды и порядок проведения анализа защищенности автоматизированных систем и их программного обеспечения
	ОПК-7.3..2 Умеет выбирать программное и аппаратное обеспечение для проведения анализа защищённости автоматизированных систем	Умеет выбирать программное обеспечение для проведения анализа защищённости автоматизированных систем
	ОПК-7.3..3 Владеет навыками проведения анализа защищенности и верификации программного обеспечения автоматизированных систем	Владеет навыками верификации программного обеспечения автоматизированных систем

3 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина(модуль) «Низкоуровневый анализ машинного кода» изучается на 4 курсе в 8 семестре.

Дисциплина является базовой дисциплиной, входит в состав блока 1 «Дисциплины (модули)» и относится к обязательным дисциплинам.

Для освоения дисциплины необходимы знания, умения, навыки и (или) опыт практической деятельности, сформированные в процессе изучения дисциплин / практик: Анализ защищенности распределенных информационных систем.

Знания, умения и навыки, сформированные при изучении дисциплины форензика, при подготовке к процедуре защиты и защите выпускной квалификационной работы.

Дисциплина «Низкоуровневый анализ машинного кода» частично реализуется в форме практической подготовки. Практическая подготовка организуется путем выполнения лабораторных работ.

Дисциплина «Низкоуровневый анализ машинного кода» в рамках воспитательной работы направлена на формирование у обучающихся умения аргументировать, самостоятельно мыслить, развивает профессиональные умения, ответственности за выполнение учебно-производственных заданий.

4 Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 3 зачетные единицы, 108 академических часов.

Распределение объема дисциплины (модуля) по видам учебных занятий представлено в таблице 2.

Таблица 2 – Объем дисциплины (модуля) по видам учебных занятий

Объем дисциплины	**Всего академических часов**
Общая трудоемкость дисциплины	108
Контактная аудиторная работа обучающихся с преподавателем (по видам учебных занятий), всего	64
В том числе:	
занятия лекционного типа (лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации педагогическими работниками)	32
занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия)	32
Самостоятельная работа обучающихся и контактная работа, включающая групповые консультации, индивидуальную работу обучающихся с преподавателями (в том числе индивидуальные консультации); взаимодействие в электронной информационно-образовательной среде вуза	44
Промежуточная аттестация обучающихся – Зачет с оценкой	

5 Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебной работы

Таблица 3 – Структура и содержание дисциплины (модуля)

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
	Контактная работа преподавателя с обучающимися			СРС
	Лекции	Семинарские (практические занятия)	Лабораторные занятия	
Основы организации ЭВМ Тема 1. История развития языков программирования Основные исторические этапы развития языков программирования (ЯП). Иерархия ЯП и	16		16 (4*)	22

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
	Контактная работа преподавателя с обучающимися			СРС
	Лекции	Семинарские (практические занятия)	Лабораторные занятия	
место языка ассемблер среди них. Роспатент, основные функции, регистрация программ для эвм Тема 2. Основы языка ассемблер и его сфера применения Синтаксис языка ассемблер. Регистры процессора Intel 8086. Команды для работы с регистрами, данными и стеком. Написание первой программы для 16-ти битной архитектуры. Работа с прерываниями. Знакомство с таблицей векторов прерывания. Применение знаний языка ассемблер при обратной разработке программного обеспечения. Отладчики и дизассемблеры для различных архитектур Тема 3. Виды синтаксисов языка ассемблер Разбор синтаксисов AT&T и Intel и их сравнение. Обзор диалектов NASM, TASM, FASM и т.д. Тема 4. Язык ассемблер для 16-ти, 32-х и 64-х битных архитектур На примере процессора Intel 8086 разбор 16-ти битной архитектуры ассемблера. Обзор 32-х битной архитектуры на примере Intel 80386. Разбор 64-х битной архитектуры на примере AMD 64. Общее сравнение архитектур. Задание 1. Отладка и дизассемблирование 16 разрядного приложения Задание 2. Отладка OllyDbg Задание 3. Отладка X64Dbg Задание 4. Отладка и дизассемблирование с IDA				
Низкоуровневый анализ машинного кода Тема 5. Обратная разработка программ, написанных на высокоуровневых языках программирования, без использования исходных кодов Краткий обзор современных дизассемблеров и отладчиков программ. Пример обратной разработки программы для получения секретного ключа, сокрытого в программе. Тема 6. Возможности языка ассемблер,	16		16 (4*)	22

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
	Контактная работа преподавателя с обучающимися			СРС
	Лекции	Семинарские (практические занятия)	Лабораторные занятия	
усложняющие обратную разработку Обзор некоторых возможностей, препятствующих статическому анализу кода. Углубленная работа со стеком, памятью и сегментом кода. Обфускация программного кода. Тема 7. Резидентные программы Краткая характеристика резидентных программ. Их отличия от обычных программ. Примеры резидентных программ. Обзор некоторых вирусов, работающих с оперативной памятью. Драйвера и приложения уровня ядра. Тема 8. Работа с таблицами векторов прерывания Обзор таблицы векторов прерывания. Возможность переписывания векторов прерывания. Пример переписывания вектора прерывания, для противодействия отладки программы. Прерывания защищенного режима работы микропроцессора. Тема 9. Работа с графикой Использование ассемблера для работы с графикой. Работа с графикой посредством прерываний. Работа с графикой напрямую, используя графическую память. Графические компоненты приемы отладки используя точки останова на API функциях. Задание 5. d2k2_crackme01, отладка, патч, кейген Задание 6. crackme01_x64.exe, отладка, патч, кейген Задание 7. crackmes.de, отладка, патч, кейген Задание 8. Отладка приложения требующего ввода пароля				
ИТОГО по дисциплине	**32**		**32**	**44**

6 Оценочные средства для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации представлен в Приложении 1.

Полный комплект контрольных заданий или иных материалов, необходимых для оценивания результатов обучения по дисциплине (модулю), практике хранится на кафедре-разработчике в бумажном и электронном виде. В пятом восьмом проведение текущего и промежуточного контроля осуществляется с использованием элементов дистанционного обучения – курс «Обратная разработка программ» на портале ДО КнАГУ.

7 Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1 Основная литература

1 Зубков, С. В. Assembler. Для DOS, Windows и Unix [Электронный ресурс] / С. В. Зубков. - М.: ДМК, 2008. -640 с. //ZNANIUM.COM : электронно-библиотечная система. – Режим доступа: http://www.znanium.com/catalog.php, ограниченный. – Загл. С экрана.

2 Лошманов А.Ю. Языки, технологии и методы программирования. Изд. - ИП Трещев И.А., г. Комсомольск-на-Амуре ISBN 978-5-4496-4768-9, 2019 – 104с.

7.2 Дополнительная литература

1 Аблязов, Р. З. Программирование на ассемблере на платформе x86-64 [Электронный ресурс] / Аблязов Р.З. - М.: ДМК, 2011. -304 с. //ZNANIUM.COM : электронно-библиотечная система. – Режим доступа: http://www.znanium.com/catalog.php, ограниченный. – Загл. С экрана.

2 Трещев И.А., Ватолина А.С., Сериков В.А. Низкоуровневый анализ машинного кода / Издательские решения, 2021. — 264 с. 978-5-0051-9307-0.

7.3 Методические указания для студентов по освоению дисциплины

Обучение дисциплине «Низкоуровневый анализ машинного кода» предполагает изучение курса на аудиторных занятиях и в ходе самостоятельной работы. Аудиторные занятия проводятся в форме лекций и лабораторных занятий. Так же используются элементы смешанного обучения – привлекаются дистанционные технологии (портал ДО КнАГУ).

Таблица 7 Методические указания к отдельным видам деятельности

Вид учебного занятия	Организация деятельности студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения. Выделять ключевые слова, формулы, отмечать на полях уточняющие вопросы по теме занятия
Лабораторные занятие	Работа с автоматизированными рабочими местами.
Самостоятельная работа	Для более глубокого изучения разделов дисциплины предусмотрены отдельные виды самостоятельной работы: подготовка к лабораторным занятиям, изучение теоретических раз-

	делов дисциплины, подготовка РГР.

Самостоятельная работа является наиболее продуктивной формой образовательной и познавательной деятельности студента в период обучения. СРС направлена на углубление и закрепление знаний студента, развитие практических умений. СРС по дисциплине «Низкоуровневый анализ машинного кода» включает следующие виды работ:

– работу с лекционным материалом, поиск и обзор литературы и электронных источников информации по индивидуальному заданию;

– опережающую самостоятельную работу;

– изучение тем, вынесенных на самостоятельную проработку;

– подготовку к практическим занятиям;

– выполнение и оформление РГР.

Контроль самостоятельной работы студентов и качество освоения дисциплины осуществляется посредством:

– представления в указанные контрольные сроки результатов выполнения заданий для текущего контроля;

– выполнения и защиты РГР;

Расчетно-графические работы должны быть оформлены в соответствии с требованиями внутренних нормативных документов ФГБОУ ВО КнАГУ.

7.4 Современные профессиональные базы данных и информационные справочные системы, используемые при осуществлении образовательного процесса по дисциплине

1. Электронно-библиотечная система ZNANIUM.COM – http://www. znanium.com.
2. Консультант+

7.5 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

1. Научная электронная библиотека Elibrary http://elibrary.ru.

С целью повышения качества ведения образовательной деятельности в университете создана электронная информационно-образовательная среда. Она подразумевает организацию взаимодействия между обучающимися и преподавателями через систему личных кабинетов студентов, расположенных на официальном сайте университета в информационно-телекоммуникационной сети «Интернет» по адресу https://student.knastu.ru. Созданная информационно-образовательная среда позволяет осуществлять взаимодействие между участниками образовательного процесса посредством организации дистанционного консультирования по вопросам выполнения практических заданий. Материалы данного курса (8 семестр) выложены на портал ДО КнАГУ и организация взаимодействия в рамках данной дисциплины проводится с привлечением дистанционных технологий.

7.6 Лицензионное программное обеспечение, используемое при осуществлении образовательного процесса по дисциплине

Таблица 5 – Перечень используемого программного обеспечения

Наименование ПО	Реквизиты
Microsoft® Windows Professional 7 Russian	Лицензионный сертификат № 46243844 от 09.12.2009

Для разработки программ рекомендуется использовать текстовый процессор Note-

pad++ (https://notepad-plus-plus.org). Для анализа и отладки программ рекомендуется AFD Pro (http://old-dos.ru/index.php?page=files&mode
=files&do=show&id=193). Для отладки программ, написанных для 32-х или 64-х битных архитектур рекомендуется использовать GDB (https://www.gnu.org/software/gdb/). Для эмулирования операционной системы MS-DOS рекомендуется использовать эмулятор DosBox (https://www.dosbox.com).

8 Организационно-педагогические условия

Организация образовательного процесса регламентируется учебным планом и расписанием учебных занятий. Язык обучения (преподавания) — русский. Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут.

При формировании своей индивидуальной образовательной траектории обучающийся имеет право на перезачет соответствующих дисциплин и профессиональных модулей, освоенных в процессе предшествующего обучения, который освобождает обучающегося от необходимости их повторного освоения.

9.1 Образовательные технологии

Учебный процесс при преподавании курса основывается на использовании традиционных, инновационных и информационных образовательных технологий. Традиционные образовательные технологии представлены лекциями и семинарскими (практическими) занятиями. Инновационные образовательные технологии используются в виде широкого применения активных и интерактивных форм проведения занятий. Информационные образовательные технологии реализуются путем активизации самостоятельной работы студентов в информационной образовательной среде.

9.2 Занятия лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов учебного плана.

На первой лекции лектор обязан предупредить студентов, применительно к какому базовому учебнику (учебникам, учебным пособиям) будет прочитан курс.

Лекционный курс должен давать наибольший объем информации и обеспечивать более глубокое понимание учебных вопросов при значительно меньшей затрате времени, чем это требуется большинству студентов на самостоятельное изучение материала.

9.3 Занятия семинарского типа

Семинарские занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы.

Основной формой проведения семинаров является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также разбор примеров и ситуаций в аудиторных условиях. В обязанности преподавателя входят: оказание методической помощи и консультирование студентов по соответствующим темам курса.

Активность на семинарских занятиях оценивается по следующим критериям:

- ответы на вопросы, предлагаемые преподавателем;
- участие в дискуссиях;
- выполнение проектных и иных заданий;
- ассистирование преподавателю в проведении занятий.

Ответ должен быть аргументированным, развернутым, не односложным, содержать ссылки на источники.

Доклады и оппонирование докладов проверяют степень владения теоретическим материалом, а также корректность и строгость рассуждений.

Оценивание заданий, выполненных на семинарском занятии, входит в накопленную оценку.

9.4 Самостоятельная работа обучающихся по дисциплине (модулю)

Самостоятельная работа студентов – это процесс активного, целенаправленного приобретения студентом новых знаний, умений без непосредственного участия преподавателя, характеризующийся предметной направленностью, эффективным контролем и оценкой результатов деятельности обучающегося.

Цели самостоятельной работы:

· систематизация и закрепление полученных теоретических знаний и практических умений студентов;

· углубление и расширение теоретических знаний;

· формирование умений использовать нормативную и справочную документацию, специальную литературу;

· развитие познавательных способностей, активности студентов, ответственности и организованности;

· формирование самостоятельности мышления, творческой инициативы, способностей к саморазвитию, самосовершенствованию и самореализации;

· развитие исследовательских умений и академических навыков.

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, уровня сложности, конкретной тематики.

Технология организации самостоятельной работы студентов включает использование информационных и материально-технических ресурсов университета.

Контроль результатов внеаудиторной самостоятельной работы студентов может проходить в письменной, устной или смешанной форме.

Студенты должны подходить к самостоятельной работе как к наиважнейшему средству закрепления и развития теоретических знаний, выработке единства взглядов на отдельные вопросы курса, приобретения определенных навыков и использования профессиональной литературы.

В данной дисциплине в рамках самостоятельной работы студенты выполняют расчетно-графическую работу.

9.5 Методические указания для обучающихся по освоению дисциплины

При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации:

1. Изучение учебной дисциплины должно вестись систематически.

2. После изучения какого-либо раздела по учебнику или конспектным материалам рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела.

3. Особое внимание следует уделить выполнению отчетов по практическим занятиям и индивидуальным комплексным заданиям на самостоятельную работу.

4. Вся тематика вопросов, изучаемых самостоятельно, задается на лекциях преподавателем. Им же даются источники (в первую очередь вновь изданные в периодической научной литературе) для более детального понимания вопросов, озвученных на лекции.

При самостоятельной проработке курса обучающиеся должны:

· просматривать основные определения и факты;

· повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной по данной теме литературы;

· изучить рекомендованную литературу, составлять тезисы, аннотации и конспекты наиболее важных моментов;

· самостоятельно выполнять задания, аналогичные предлагаемым на занятиях;

· использовать для самопроверки материалы фонда оценочных средств.

1. Методические указания при работе над конспектом лекции

В ходе лекционных занятий необходимо вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

2. Методические указания по самостоятельной работе над изучаемым материалом и при подготовке к лабораторным занятиям

Начинать надо с изучения рекомендованной литературы. Необходимо помнить, что на лекции обычно рассматривается не весь материал, а только его часть. Остальная его часть восполняется в процессе самостоятельной работы. В связи с этим работа с рекомендованной литературой обязательна. Особое внимание при этом необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического приложения рассматриваемых теоретических вопросов. В процессе этой работы необходимо стремиться понять и запомнить основные положения рассматриваемого материала, примеры, поясняющие его, а также разобраться в иллюстративном материале. Оформлять отчеты следует руководствуясь внутренними нормативными документами КнАГУ.

3. Методические указания по выполнению расчетно-графической работы

Теоретическая часть расчетно-графической работы выполняется по установленным темам с использованием практических материалов. К каждой теме расчетно-графической работы рекомендуется примерный перечень узловых вопросов, список необходимой литературы. Излагая вопросы темы, следует строго придерживаться плана. Работа не должна представлять пересказ отдельных глав учебника или учебного пособия. Необходимо изложить собственные соображения по существу излагаемых вопросов, внести свои предложения. Общие положения должны быть подкреплены и пояснены конкретными примерами. Излагаемый материал при необходимости следует проиллюстрировать таблицами, схемами, диаграммами.

9 Описание материально-технического обеспечения, необходимого для осуществления образовательного процесса по дисциплине (модулю)

9.1 Учебно-лабораторное оборудование

Таблица 6 – Перечень оборудования лаборатории

Аудитория	Наименование аудитории (лаборатории)	Используемое оборудование
202/5	Лаборатория программно-аппаратных средств защиты информации	СЗИ НСД Secret Net, СЗИ НСД Dallas Lock, СЗИ НСД Страж NT, СЗИ НСД Щит РЖД, СЗИ НСД Аура ,СЗИ НСД Криптон ,СЗИ НСД Аккорд, ФИКС, Ревизор 1,2 как для операционных систем семейства Windows так и для Linux, Ревизор Сети 2.0, Анализатор сетевого траффика Астра,Агент инвентаризации сети,Сканер сетевой безопасности XSpider, Терьер, Secret Net Touch Memory Card, Криптон АМДЗ, Аккорд АМДЗ, КриптоПРО АРМ, ,CryptoPro CSP 3.6, VipNet firewall, Etoken PKI Client, Etoken, Ноутбук с Windows 7+проектор. 16 ПЭВМ на базе процессоров не ниже Intel Pentium IV

9.2 Технические и электронные средства обучения

Лекционные занятия

Аудитории для лекционных занятий укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории (наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук), учебно-наглядные пособия, тематические иллюстрации).

Лабораторные занятия

Для лабораторных занятий используется аудитория №_202_, оснащенная оборудованием, указанным в табл. 8:

Самостоятельная работа.

Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде КнАГУ:

- читальный зал НТБ КнАГУ;
- компьютерные классы (ауд. 311 корпус № 5, ауд. 205 корпус № 5, ауд. 313 корпус № 5).

11 Иные сведения

Методические рекомендации по обучению лиц с ограниченными возможностями здоровья и инвалидов

Освоение дисциплины обучающимися с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах. Предполагаются специальные условия для получения образования обучающимися с ограниченными возможностями здоровья.

Профессорско-педагогический состав знакомится с психолого-физиологическими особенностями обучающихся инвалидов и лиц с ограниченными возможностями здоровья, индивидуальными программами реабилитации инвалидов (при наличии). При необходимости осуществляется дополнительная поддержка преподавания тьюторами, психологами, социальными работниками, прошедшими подготовку ассистентами.

В соответствии с методическими рекомендациями Минобрнауки РФ (утв. 8 апреля 2014 г. N АК-44/05вн) в курсе предполагается использовать социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе. Подбор и разработка учебных материалов производятся с учетом предоставления материала в различных формах: аудиальной, визуальной, с использованием специальных технических средств и информационных систем.

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения (персонального и коллективного использования). Материально-техническое обеспечение предусматривает приспособление аудиторий к нуждам лиц с ОВЗ.

Форма проведения аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей. Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

· в печатной или электронной форме (для лиц с нарушениями опорно-двигательного аппарата);

· в печатной форме или электронной форме с увеличенным шрифтом и контрастностью (для лиц с нарушениями слуха, речи, зрения);

· методом чтения ассистентом задания вслух (для лиц с нарушениями зрения).

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

· письменно на бумаге или набором ответов на компьютере (для лиц с нарушениями слуха, речи);

· выбором ответа из возможных вариантов с использованием услуг ассистента (для лиц с нарушениями опорно-двигательного аппарата);

· устно (для лиц с нарушениями зрения, опорно-двигательного аппарата).

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ[1]
по дисциплине

Низкоуровневый анализ машинного кода

Направление подготовки	*10.05.03 "Информационная безопасность автоматизированных систем"*
Направленность (профиль) образовательной программы	*Анализ безопасности информационных систем*
Квалификация выпускника	*специалист по защите информации*
Год начала подготовки *(по учебному плану)*	*2021*
Форма обучения	*очная*
Технология обучения	*традиционная*

Курс	Семестр	Трудоемкость, з.е.
4	*8*	*3*

Вид промежуточной аттестации	Обеспечивающее подразделение
Зач_с_оц	*Кафедра ИБАС - Информационная безопасность автоматизированных систем*

[1] В данном приложении представлены типовые оценочные средства. Полный комплект оценочных средств, включающий все варианты заданий (тестов, контрольных работ и др.), предлагаемых обучающемуся, хранится на кафедре в бумажном и электронном виде.

1 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами образовательной программы

Таблица 1 – Компетенции и индикаторы их достижения

Код и наименование компетенции	Индикаторы достижения	Планируемые результаты обучения по дисциплине
Общепрофессиональные		
ОПК-7.3. Способен проводить анализ защищенности и верификацию программного обеспечения информационных систем	**ОПК-7.3..1** Знает виды и порядок проведения анализа защищенности автоматизированных систем	Знает виды и порядок проведения анализа защищенности автоматизированных систем и их программного обеспечения
	ОПК-7.3..2 Умеет выбирать программное и аппаратное обеспечение для проведения анализа защищённости автоматизированных систем	Умеет выбирать программное обеспечение для проведения анализа защищённости автоматизированных систем
	ОПК-7.3..3 Владеет навыками проведения анализа защищенности и верификации программного обеспечения автоматизированных систем	Владеет навыками верификации программного обеспечения автоматизированных систем

Таблица 2 – Паспорт фонда оценочных средств

Контролируемые разделы (темы) дисциплины	**Формируемая компетенция**	**Наименование оценочного средства**	**Показатели оценки**
Тема 1. История развития языков программирования	**ОПК-7.3**	Лабораторная работа 1	Знает основные исторические этапы развития языков программирования. Представляет иерархию языков программирования. Называет место языка ассемблер среди языков программирования.
Тема 2. Основы языка ассемблер и его сфера применения	**ОПК-7.3**	Лабораторная работа 2	Знает синтаксис языка ассемблер. Имеет представление о регистрах процессора Intel 8086. Называет команды для работы с регистрами, данными и стеком.

			Владеет навыками написания простейших программ. Демонстрирует навыки при работе с прерываниями. Знаком с таблицей векторов прерывания. Применяет знания языка ассемблер при обратной разработке программного обеспечения.
Тема 3. Виды синтаксисов языка ассемблер	**ОПК-7.3**	Лабораторная работа 3	Способен ориентироваться в синтаксисах AT&T и Intel. Владеет базовым пониманием диалектов NASM, TASM, FASM и т.д.
Тема 4. Язык ассемблер для 16-ти, 32-х и 64-х битных архитектур	**ОПК-7.3**	Лабораторная работа 4	Владеет знаниями о 16-ти битной архитектуре ассемблера. Проводит аналогию между различными архитектурами ассемблера. Демонстрирует знания при анализе программ для 16-ти, 32-х и 64-х битных архитектур.
Тема 5. Обратная разработка программ, написанных на высокоуровневых языках программирования, без использования исходных кодов	**ОПК-7.3**	Лабораторная работа 5	Знает современные дизассемблеры и отладчики программ. Способен отлаживать и дизассемблировать программы без использования исходных кодов. Имеет представление об основных высокоуровневых конструкциях языков программирования.
Тема 6. Возможности языка ассемблер, усложняющие обратную разработку	**ОПК-7.3**	Лабораторная работа 6	Называет возможности, препятствующие статическому анализу кода.

			Способен использовать теоретические знания в практической деятельности. Демонстрирует навыки глубокого понимания работы стека, памяти, кода и т.д.
Тема 7. Резидентные программы	**ОПК-7.3**	Лабораторная работа 7	Способен назвать характеристики резидентных программ. Имеет представление о работе резидентных программ Владеет навыками написания простейших резидентных программ. Показывает способность отличать резидентную программу от нерезидентной по ее исходному коду и поведению.
Тема 8. Работа с таблицами векторов прерывания	**ОПК-7.3**	Лабораторная работа 8	Знает общие сведения о таблице векторов прерывания. Способен переписывать векторы прерывания. Демонстрирует навыки работы с таблицами векторов прерывания для противодействия отладке.
Тема 9. Работа с графикой	**ОПК-7.3**	Лабораторная работа 8	Умеет применять ассемблер для построения графического изображения. Знает различия между системными прерываниями и использованием графической памяти при работе с графикой. Демонстрирует навыки работы с си-

			стемными прерываниями и прямым доступом к памяти при разработке игры.
Все темы	**ОПК-7.3**	РГР	Практическая часть РГР выполнена верно.

2 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций

Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, представлены в виде технологической карты дисциплины (таблица 3).

Таблица 6 – Технологическая карта

	Наименование оценочного средства	**Сроки выполнения**	**Шкала оценивания**	**Критерии оценивания**
8 семестр ***Промежуточная аттестация в форме Зач_с_оц***				
1	Лабораторная работа 1	3 неделя	15	0 баллов – задание не выполнено или выполнено не верно 5 балла – задание выполнено с недочетами и не в срок 10 балла – задание выполнено без недочетов и не в срок 15 баллов – задание выполнено без недочетов и в срок
2	Лабораторная работа 2	6 неделя	15	0 баллов – задание не выполнено или выполнено не верно 5 балла – задание выполнено с недочетами и не в срок 10 балла – задание выполнено без недочетов и не в срок 15 баллов – задание выполнено без недочетов и в срок
3	Лабораторная работа 3	9 неделя	15	0 баллов – задание не выполнено или выполнено не верно 5 балла – задание выполнено с недочетами и не в срок 10 балла – задание выполнено без недочетов и не в срок

	Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
				15 баллов – задание выполнено без недочетов и в срок
4	Лабораторная работа 4	12 неделя	15	0 баллов – задание не выполнено или выполнено не верно 5 балла – задание выполнено с недочетами и не в срок 10 балла – задание выполнено без недочетов и не в срок 15 баллов – задание выполнено без недочетов и в срок
5	Лабораторная работа 5	15 неделя	15	0 баллов – задание не выполнено или выполнено не верно 5 балла – задание выполнено с недочетами и не в срок 10 балла – задание выполнено без недочетов и не в срок 15 баллов – задание выполнено без недочетов и в срок
5	Лабораторная работа 6	15 неделя	15	0 баллов – задание не выполнено или выполнено не верно 5 балла – задание выполнено с недочетами и не в срок 10 балла – задание выполнено без недочетов и не в срок 15 баллов – задание выполнено без недочетов и в срок
5	Лабораторная работа 7	15 неделя	15	0 баллов – задание не выполнено или выполнено не верно 5 балла – задание выполнено с недочетами и не в срок 10 балла – задание выполнено без недочетов и не в срок 15 баллов – задание выполнено без недочетов и в срок
5	Лабораторная работа 8	15 неделя	15	0 баллов – задание не выполнено или выполнено не верно

	Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
				5 балла – задание выполнено с недочетами и не в срок 10 балла – задание выполнено без недочетов и не в срок 15 баллов – задание выполнено без недочетов и в срок
9	Расчетно-графическая работа	17 неделя	25	0 баллов – задание не выполнено или выполнено не верно 5 балла – задание выполнено с недочетами и не в срок 15 балла – задание выполнено без недочетов и не в срок 25 баллов – задание выполнено без недочетов и в срок
ИТОГО Текущий контроль:		-	145 баллов	-
Критерии оценки результатов обучения по дисциплине: 0 – 64 % от максимально возможной суммы баллов – «неудовлетворительно» (недостаточный уровень для промежуточной аттестации по дисциплине); 65 – 74 % от максимально возможной суммы баллов – «удовлетворительно» (пороговый (минимальный) уровень); 75 – 84 % от максимально возможной суммы баллов – «хорошо» (средний уровень); 85 – 100 % от максимально возможной суммы баллов – «отлично» (высокий (максимальный) уровень)				

3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций в ходе освоения образовательной программы

3.1 Задания для текущего контроля успеваемости

Задания для дисциплины представлены на портале ДО КнАГУ.

Пример задания на лабораторную работу 1

Вам выдан рабочий модуль программы (COM файл). При запуске этой программы производится запрос пароля, после чего дается заключение о правильности прохода через пароль. Ваша задача:

Используя отладчик AFD или TD пройти по программе, найти место, где происходит дешифровка пароля и расшифровать его, после чего снова запустить программу, ввести правильный пароль и получить подтверждение о правильности прохода через пароль.

Используя дизассемблер SOUSER

дизассемблировать выданную программу

автоматически построить блок схему алгоритма ее работы

найти в тексте программы место проверки пароля и подавить проверку

заново ассемблировать программу и представить ее преподавателю, продемонстрировав, что программа теперь не запрашивает пароль (или успешно завершается при лю-

бом пароле).

Оформить электронный отчет, в котором отразить:

титульный лист;

тему лабораторной работы и задание на лабораторную работу;

описание этапов дешифровки пароля и экранные формы отладчика, использованные при дешифровке пароля;

описание этапов дизассемблирования программы и экранные формы дизассемблера, использованные при этом, в отчет включить УЧАСТОК дизассемблированной программы, в котором происходит дешифровка и обработка пароля;

описание этапов автоматического построения блок-схемы алгоритма программы, в отчет включить УЧАСТОК блок-схемы алгоритма, в котором происходит дешифровка и обработка пароля;

описание приемов, примененных для подавления обработки пароля, в отчет включить УЧАСТОК дизассемблированной программы измененный Вами с целью подавления обработки пароля;

описание порядка ассемблирования программы;

вид экрана после срабатывания откорректированной программы;

Пример задания на лабораторную работу 2

Описать функционал приложения по отладке программного обеспечения OllyDbg. Обязательно подробно описать одну из функций, не пересекаясь с другими студентами из группы по описываемой функции. Пример функции ссылки.

Пример задания на лабораторную работу 3

Описать функционал приложения по отладке программного обеспечения X64Dbg. Обязательно подробно описать одну из функций, не пересекаясь с другими студентами из группы по описываемой функции пример функции ссылки. Обязательно найти отличия не пересекающиеся с другими студентами

Пример задания на лабораторную работу 4

Описать функционал приложения по отладке программного обеспечения IDA Free. Обязательно подробно описать одну из функций, например построение дерева обхода, не пересекаясь с другими студентами из группы по описываемой функции.

Пример задания на лабораторную работу 5

Варианты получить файл d2k2_crackme01 (1)

1. Изменить 1 байт продемонстрировать что программа приняла серийный номер.
2. Изменить ключевой условный переход
3. Изменить ключевой безусловный переход
4. Описать процесс формирования серийного номера.
5. Описать процесс распаковки серийного номера.
6. Изменить 2 байта продемонстрировать что программа приняла серийный номер
7. Построить граф работы программы
8. Исследовать и определить длины серийного номера, имени
9. Исследовать и определить адерса имени и серийного номера
10. Изменить произвольное количество байт (более 2), продемонстрировать что программа приняла серийный номер
11. Определить константы для упаковки серийного номера
12. Определить ключевые участки кода ответственные за упаковку серийного номера.
13. Определить константы для распаковки серийного номера
14. Определить константы для распаковки серийного номера
15.* Получить действительную пару имя, серийный номер (это задание может сделать любой если затрудняется сделать свой вариант)

16.* Написать патч для приложения (это задание может сделать любой если затрудняется сделать свой вариант)
17.** Написать кейген для приложения(это задание может сделать любой если затрудняется сделать свой вариант).
Дополнительно. На портале ДО ФГБОУ ВО КнАГУ приведен файл задание с rootme.org. Необходимо выполнить задание в рамках данной лабораторной работы (получить пароль).

Пример задания на лабораторную работу 6

Получить файл crackme01_x64.exe
Варианты
1. Изменить 1 байт продемонстрировать что программа приняла серийный номер.
2. Изменить ключевой условный переход
3. Изменить ключевой безусловный переход
4. Описать процесс формирования серийного номера.
5. Описать процесс распаковки серийного номера.
6. Изменить 2 байта продемонстрировать что программа приняла серийный номер
7. Построить граф работы программы
8. Исследовать и определить длины серийного номера, имени
9. Исследовать и определить адерса имени и серийного номера
10. Изменить произвольное количество байт (более 2), продемонстрировать что программа приняла серийный номер
11. Определить константы для упаковки серийного номера
12. Определить ключевые участки кода ответственные за упаковку серийного номера.
13. Определить константы для распаковки серийного номера
14. Определить константы для распаковки серийного номера
15.* Получить действительную пару имя, серийный номер (это задание может сделать любой если затрудняется сделать свой вариант)
16.* Написать патч для приложения (это задание может сделать любой если затрудняется сделать свой вариант)
17.** Написать кейген для приложения(это задание может сделать любой если затрудняется сделать свой вариант).

Пример задания на лабораторную работу 7

Получить файл level_2.exe
Варианты
1. Изменить 1 байт продемонстрировать что программа приняла серийный номер.
2. Изменить ключевой условный переход
3. Изменить ключевой безусловный переход
4. Описать процесс формирования серийного номера.
5. Описать процесс распаковки серийного номера.
6. Изменить 2 байта продемонстрировать что программа приняла серийный номер
7. Построить граф работы программы
8. Исследовать и определить длины серийного номера, имени
9. Исследовать и определить адерса имени и серийного номера
10. Изменить произвольное количество байт (более 2), продемонстрировать что программа приняла серийный номер
11. Определить константы для упаковки серийного номера
12. Определить ключевые участки кода ответственные за упаковку серийного номера.
13. Определить константы для распаковки серийного номера
14. Определить константы для распаковки серийного номера
15.* Получить действительную пару имя, серийный номер (это задание может сделать любой если затрудняется сделать свой вариант)

16.* Написать патч для приложения (это задание может сделать любой если затрудняется сделать свой вариант)
17.** Написать кейген для приложения(это задание может сделать любой если затрудняется сделать свой вариант).

Пример задания на лабораторную работу 8

При запуске программ производится запрос пароля (или организуется регистрация программы), после чего дается заключение о правильности прохода через пароль. Каждому студенту выдается свое приложение. Ваша задача:
Знакомство с отладчиком уровня ПРИЛОЖЕНИЯ
Используя отладчик OlleDebuger пройти по программе, найти место, где происходит дешифровка пароля и расшифровать его, после чего снова запустить программу, ввести правильный пароль и получить подтверждение о правильности прохода через пароль.
Знакомство с дизассемблером
Используя дизассемблер IDA
ознакомиться с методикой дизассемблирования Win приложений
дизассемблировать выданную программу
найти в тексте программы место проверки пароля.
исправить ассемблерный код так, чтобы программа срабатывала при любом пароле, определить вид изменений в коде исполняемого файла
- внести изменения в код исполняемого файла любым способом, чтобы программа срабатывала при любом введенном пароле
Оформить электронный отчет, в котором отразить:
титульный лист;
тему лабораторной работы и задание на лабораторную работу;
описание этапов дешифровки пароля на OLLEDEDUGER
описание использования дизассембелра IDA
и экранные формы из дизассемблера, использованные при дешифровке пароля;
вид экрана после срабатывания откорректированной программы;

Возможные вопросы и задания для защиты работ

1. Назначение битов регистра FLAGS.
2. Регистры для 64-х битной архитектуры.
3. Бит, байт, слово, двойное слово, сегмент.
4. Компилятор и компоновщик.
5. Команды для арифметических операций.
6. Команды для логических операций.
7. Структура и принцип работы стека.
8. Назначение регистров IP, SP, BP.
9. Свойства операций умножения и деления.
10. Команды CALL и RET.
11. Основные сведения о сегменте данных и сегменте кода.
12. Системные прерывания.
13. Назначение регистров CX, BX, DX и AX.
14. Способы адресации.
15. Команды условного и безусловного переходов.
16. Команды сравнения.
17. Команды цикла.
18. Команды сдвиги и циклического сдвига.
19. Назначение регистров CS, DS, ES, SS.
20. Размерность команд и регистров.

Комплект заданий для расчетно-графической работы

Расчетно-графическая работа студента представляет из себе реверс-инжиниринг реального приложения. Для разбора необходимо брать не актуальные версии приложений, которые больше не поддерживаются производителями и для которых с точки зрения законодательства реверс разрешен только в ознакомительных целях и только в условиях лабораторатоных испытаний. Для каждого студента обязательно согласовать наименование программного обеспечения с преподавателем. Примеры выбора приложений:

1. WinRar 1.0
2. KMPlayer 1.0
3. UltraIso 1.0
4. WinAmp 1.0
5. Visual Prolog 5.0
6. WinZip 1.0

Оформить отчет по проделанной работе.

Лист регистрации изменений к РПД

	Номер протокола заседания кафедры, дата утверждения изменения	Количество страниц изменения	Подпись разработчика РПД