

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

УТВЕРЖДАЮ

Декан факультета ____ Трешев И.А. ____

ФИО декана

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Низкоуровневый анализ машинного кода»

Специальность	10.05.03 Информационная безопасность автоматизированных систем
Специализация	Анализ безопасности информационных систем

Обеспечивающее подразделение
Кафедра «Информационная безопасность автоматизированных систем»

Комсомольск-на-Амуре 2023

Разработчик рабочей программы:

Доцент, к.т.н.

(должность, степень, ученое звание)



(подпись)

Трещев И.А.

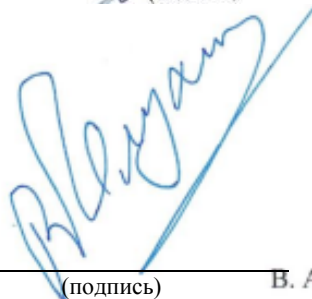
(ФИО)

СОГЛАСОВАНО:

Заведующий кафедрой

ИБАС

(наименование кафедры)



(подпись)

В. А. Челухин (ФИО)

1 Общие положения

Рабочая программа и фонд оценочных средств дисциплины «Низкоуровневый анализ машинного кода» составлены в соответствии с требованиями федерального государственного образовательного стандарта, утвержденного приказом Минобрнауки Российской Федерации от 26.11.2020 №1457, и основной профессиональной образовательной программы подготовки «Анализ безопасности информационных систем» по специальности «10.05.03 Информационная безопасность автоматизированных систем».

Задачи дисциплины	<ul style="list-style-type: none">• 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:

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 ОПК-7.3..2 Умеет выбирать программное и аппаратное обеспечение для проведения анализа защищенности автоматизированных систем ОПК-7.3..3 Владеет навыками проведения анализа защищенности и верификации программного обеспечения автоматизированных систем	Знает виды и порядок проведения анализа защищенности автоматизированных систем и их программного обеспечения Умеет выбирать программное обеспечение для проведения анализа защищенности автоматизированных систем Владеет навыками верификации программного обеспечения автоматизированных систем

3 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Низкоуровневый анализ машинного кода» входит в состав блока 1 «Дисциплины (модули)» и относится к базовой части.

Место дисциплины (этап формирования компетенции) отражено в схеме формирования компетенций, представленной в документе *Оценочные материалы*, размещенном на сайте университета www.knastu.ru / *Наш университет* / *Образование* / *10.05.03 Информационная безопасность автоматизированных систем* / *Оценочные материалы*).

Дисциплина «Низкоуровневый анализ машинного кода» частично реализуется в форме практической подготовки. Практическая подготовка организуется путем проведения, лабораторных работ, выполнения курсовых/ работ, иных видов учебной деятельности.

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

4.1 Структура и содержание дисциплины для очной формы обучения

Дисциплина «Низкоуровневый анализ машинного кода» изучается на 4 курсе, 8 семестре.

Общая трудоёмкость дисциплины составляет 3 з.е., 108 ч., в том числе контактная работа обучающихся с преподавателем 64 ч., промежуточная аттестация в форме зачета с оценкой., самостоятельная работа обучающихся 44 ч.

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)					
	Контактная работа преподавателя с обучающимися			ИКР	Пром. аттест.	СРС
	Лекции	Практические занятия	Лабораторные работы			
<p>Основы организации ЭВМ</p> <p>Тема 1. История развития языков программирования</p> <p>Основные исторические этапы развития языков программирования (ЯП). Иерархия ЯП и место языка ассемблер среди них. Роспатент, основные функции, регистрация программ для эвм</p> <p>Тема 2. Основы языка ассемблер и его сфера применения</p> <p>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 архи-</p>	16		16			22

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)					
	Контактная работа преподавателя с обучающимися			ИКР	Пром. аттест.	СРС
	Лекции	Практические занятия	Лабораторные работы			
<p>текстур</p> <p>Тема 3. Виды синтаксисов языка ассемблер</p> <p>Разбор синтаксисов AT&T и Intel и их сравнение. Обзор диалектов NASM, TASM, FASM и т.д.</p> <p>Тема 4. Язык ассемблер для 16-ти, 32-х и 64-х битных архитектур</p> <p>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.</p> <p>Общее сравнение архитектур.</p> <p>Задание 1. Отладка и дизассемблирование 16 разрядного приложения</p> <p>Задание 2. Отладка OllyDbg</p> <p>Задание 3. Отладка X64Dbg</p> <p>Задание 4. Отладка и дизассемблирование с IDA</p>						
<p>Низкоуровневый анализ машинного кода</p> <p>Тема 5. Обратная разработка программ, написанных на высокоуровневых языках программирования, без использования исходных кодов</p> <p>Краткий обзор современных дизассемблеров и отладчиков программ. Пример обратной разработки программы для получения секретного ключа, сокрытого в программе.</p> <p>Тема 6. Возможности языка ассемблер, усложняющие обратную разработку</p> <p>Обзор некоторых возможностей, препятствующих статическому анализу кода. Углубленная работа со стеком, памятью и сегментом кода. Обфускация программного кода.</p>	16		16		22	

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)					
	Контактная работа преподавателя с обучающимися			ИКР	Пром. аттест.	СРС
	Лекции	Практические занятия	Лабораторные работы			
<p>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.</p> <p>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.</p> <p>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.</p> <p>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</p>						
<i>Зачет с оценкой</i> При наличии в учебном плане. Проводится на последнем занятии семинарского типа	-	-	-	-	-	
ИТОГО по дисциплине	32 в том числе в форме практической	-:	32 в том числе в форме практической	-	-	44

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)					
	Контактная работа преподавателя с обучающимися			ИКР	Пром. аттест.	СРС
	Лекции	Практические занятия	Лабораторные работы			
	ской подготовки: 8		подготовки: 16			

* реализуется в форме практической подготовки

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

Фонды оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации обсуждаются и утверждаются на заседании кафедры. Полный комплект контрольных заданий или иных материалов, необходимых для оценивания результатов обучения по дисциплине (модулю) хранится на кафедре-разработчике в бумажном или электронном виде, также фонды оценочных средств доступны студентам в личном кабинете – раздел учебно-методическое обеспечение.

6 Учебно-методическое и информационное обеспечение дисциплины (модуля)

6.1 Основная и дополнительная литература

Перечень рекомендуемой основной и дополнительной литературы представлен на сайте университета www.knastu.ru / *Наш университет / Образование / 10.05.03 Информационная безопасность автоматизированных систем / Рабочий учебный план / Реестр литературы.*

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

Каждому обучающемуся обеспечен доступ (удаленный доступ), в том числе в случае применения электронного обучения, дистанционных образовательных технологий, к современным профессиональным базам данных и информационным справочным системам, с которыми у университета заключен договор.

Перечень рекомендуемых профессиональных баз данных и информационных справочных систем представлен на сайте университета www.knastu.ru / *Наш университет / Образование / 10.05.03 Информационная безопасность автоматизированных систем / Рабочий учебный план / Реестр ЭБС.*

Актуальная информация по заключенным на текущий учебный год договорам приведена на странице Научно-технической библиотеки (НТБ) на сайте университета <https://knastu.ru/page/3244>

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

На странице НТБ можно воспользоваться интернет-ресурсами открытого доступа по укрупненной группе направлений и специальностей (УГНС) 10.00.00 Информационная безопасность:

<https://knastu.ru/page/539>

Название сайта	Электронный адрес
Сайты электронных фондов нормативно-технической документации по строительству	
База данных нормативных документов для строительства бесплатная).	http://www.norm-load.ru
Бесплатная информационно-справочная система онлайн доступа к полному собранию технических нормативно правовых актов РФ.	http://gostrf.com
Техноэксперт. Электронный фонд правовой и нормативно-технической документации.	http://docs.cntd.ru

7 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.

7.1 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.

7.2 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.

7.3 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.

7.4 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.

7.5 Методические рекомендации 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.

8 Материально-техническое обеспечение, необходимое для осуществления образовательного процесса по дисциплине (модулю)

8.1 Лицензионное и свободно распространяемое программное обеспечение, используемое при осуществлении образовательного процесса по дисциплине

Университет обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства. Состав программного обеспечения, необходимого для освоения дисциплины, приведен на сайте университета www.knastu.ru / *Наш университет / Образование / 10.05.03 Информационная безопасность автоматизированных систем / Рабочий учебный план / Реестр ПО.*

Актуальные на текущий учебный год реквизиты / условия использования программного обеспечения приведены на странице ИТ-управления на сайте университета:

<https://knastu.ru/page/1928>

8.2 Учебно-лабораторное оборудование

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 трафика 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

8.3 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 *(при наличии)*.

Для лабораторных занятий используется аудитория, оснащенная оборудованием, указанным в табл. п. 8.2.

Самостоятельная работа.

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

- зал электронной информации НТБ КнАГУ;
- компьютерные классы факультета.

9 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.