МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ
заведующий кафедрой
кибербезопасности
информационных систем
С.Л. Кенин

22.03.2024

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ Б1.В.ДВ.04.02 Безопасность системного программного обеспечения

1. Код и наименование направления подготовки/специальности:

10.05.01 Компьютерная безопасность

2. Профиль подготовки/специализация:

"Безопасность компьютерных систем и сетей" (по отрасли или в сфере профессиональной деятельности)

3. Квалификация (степень) выпускника: Специалист

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины:

кибербезопасности информационных систем

6. Составители программы:

Степанец Юлия Александровна, к.т.н., доцент кафедры кибербезопасности информационных систем

7. Рекомендована:
НМС факультета ПММ, протокол № 7 от 26.05.2023г.
Внесены изменения: протокол УС факультета ПММ, протокол № 8 от 27.02.2024г.
Рекомендована с изменениями: протокол НМС факультета ПМ, протокол № 5 от 22.03.2024г.

8. Учебный год: 2027/2028 **Семестр(ы):** 9

9. Цели и задачи учебной дисциплины

Целью дисциплины является изучение понятий и методов разработки программного обеспечения, способов тестирования и оценивания качества программных систем.

Задачи дисциплины: в процессе обучения студенты должны изучить терминологию, используемую при разработке программного обеспечения, усвоить методы разработки и проектирования программных систем, снижения ошибок и рисков при разработке программного обеспечения и приобрести навыки оценки сложности разрабатываемых программных комплексов.

10. Место учебной дисциплины в структуре ОПОП: дисциплина относится к вариативной части блока Б1 дисциплин учебного плана.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями) и индикаторами их достижения

Код	Название компетенции	Код(ы)	Индикаторы(ы)	Планируемые результаты обучения
ПК-1	Способен проводить анализ требований и выполнять работы по проектированию программных и аппаратных компонент системы безопасности компьютерных систем и сетей, в том числе с использованием современных методов и средств защиты информации	ПК-1.1	применяет современные методы разработки программного обеспечения и технологии программирования	Знает: современные методы разработки программного обеспечения и технологии программирования; Умеет: применять современные методы разработки программного обеспечения и технологии программирования; использовать принципы комплексной разработки правил, процедур, приемов и методов, при создании средств защиты информации, в том числе с использованием современных методов и средств разработки программного обеспечения Владеет современными методами разработки программного обеспечения и технологии программирования;
		ПК-1.3	использует принципы комплексной разработки правил, процедур, приемов и методов, при создании средств защиты информации, в том числе с использованием современных методов и средств разработки программного обеспечения	
ПК-2	Способен принимать участие в экспертизе и анализе уязвимостей, угроз и инцидентов информационной безопасности в компьютерных системах и сетях	ПК-2.1	применяет эффективные методы и средства планирования и организации исследований и разработки	Знает: эффективные методы и средства планирования и организации исследований и разработки Умеет: применяет эффективные методы и средства планирования и организации исследований и разработки
ПК-3	Способен участвовать в работах по проектированию систем защиты информации в компьютерных системах и сетях при решении профессиональных, исследовательских и прикладных задач	ПК-3.5	выполняет проверку устойчивости приложений к внешнему несанкционированному доступу, в том числе проверка устойчивости веб-приложений к атакам, применение средств контроля безопасности, управление криптографическими	Умение: выполняет проверку устойчивости приложений к внешнему несанкционированному доступу, в том числе проверка устойчивости веб-приложений к атакам, применение средств контроля безопасности, управление криптографическими средствами, а также организация мероприятий по обеспечению кибербезопасности

			средствами, а также организация мероприятий по обеспечению кибербезопасности	

12. Объем дисциплины в зачетных единицах/час - 4/144.
Форма промежуточной аттестации - зачет с оценкой.

13. Трудоемкость по видам учебной работы

Вид учебной работы	Трудоёмкость (часы)					
	Всего	В том числе в интерактивной форме	По семестрам			
			9			
Аудиторные занятия	72		72			
в том числе: лекции	36		36			
Практические	0		0			
Лабораторные	36		36			
Самостоятельная работа	72		72			
Контроль	0		0			
Итого:	144		144			
Форма промежуточной аттестации	зачет с оценкой		зачет с оценкой			

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1. Лекции			
1.1	Системное программное обеспечение. Классификация системных программ.	Системное программное обеспечение: основные понятия и их определения; расположение СПО в общей структуре ЭВМ, классификация и структура СПО; организация взаимодействия между аппаратурой ЭВМ, СПО и прикладным ПО. Классификация системных программ: операционная система, загрузчики, трансляторы, компиляторы и интерпретаторы, отладчики, утилиты. Интерфейс операционной системы: основные принципы и стандарты; системные вызовы; интерфейсы WinAPI, POSIX API; 32 и 64 разрядные интерфейсы; проблема локализации, стандарты ANSI и UNICODE.	Б1.В.ДВ.04.02 Безопасность системного программного обеспечения (10.05.01) https://edu.vsu.ru/course/
1.2	Особенности выполнения программ. Синхронизация потоков. Решение классических проблем синхронизации и реализация синхронизации	Объекты ядра: создание, уничтожение, таблица описателей, учет пользователей объектов ядра, наследование. Процесс выполнения программ: создание, завершение процессов и потоков. Синхронизация потоков: механизмы синхронизации (семафоры, мониторы, сообщения, барьеры). Решение классических проблем синхронизации: проблема обедающих философов, проблема читателей и писателей, проблема спящего брадобрея. Реализация синхронизации: синхронизация потоков в пользовательском режиме; синхронизация потоков с использованием объектов ядра. Межпроцессные взаимодействия (IPC): механизмы, каналы, очереди сообщений, разделяемые сегменты памяти, сокеты, вызов удаленных процедур (RPC).	
1.3	Ввод-вывод. Принципы работы, программные уровни вводы-вывода. Драйвера устройств	Принципы аппаратуры ввода-вывода: устройства, контроллеры устройств; ввод-вывод, отображаемый на адресное пространство памяти; прямой доступ к памяти (DMA); настройка адресов и защита. Принципы программного обеспечения ввода-вывода: задачи ПО; управляемый прерываниями ввод-вывод; ввод-вывод с использованием DMA.	

		Программные уровни ввода-вывода: обработчики прерываний, драйверы устройств, независимое от устройств ПО ввода-вывода; ПО ввода-вывода пространства пользователя. Подсистема ввода-вывода в MS Windows: компоненты ввода-вывода и их взаимодействие; объекты, осуществляющие взаимодействие; драйвера. Взаимоблокировки, безопасные и небезопасные состояния. Унифицированная модель разработки драйверов. Взаимоблокировки, их обнаружение. Избежание взаимоблокировок; безопасные и небезопасные состояния.	
1.4	Подсистема безопасности	Подсистема безопасности: цели; защита объектов. Подсистема безопасности: цели; защита объектов; аудит; права и привилегии; выполнение действий от другого имени; аутентификация. Реализация подсистемы безопасности в MS Windows и Unix: компоненты, основные принципы и механизмы защиты.	
1.5	Информационная безопасность в операционных системах и сетях.	Основные понятия безопасности информации. Каналы утечки. Объекты защиты. Возможные угрозы. Классификация угроз. Программные и аппаратные средства защиты информации. Базовые принципы организации защиты. Системный подход к организации защиты информации в компьютерных системах. Общие правила защиты. Безопасность в операционных системах. Типовая архитектура подсистемы защиты в операционных системах. Разграничение доступа к объектам ОС. Идентификация, аутентификация и авторизация субъектов доступа. Организация парольных систем (требования при выборе, хранение, передача по сети, методы подбора, защита от компрометации). Административные принципы защиты. Управление политикой безопасности. Организация защиты информации в Windows. Субъекты и объекты доступа (защиты). Понятия о правах и привилегиях. Аудит. Требования к аудиту. Политика аудита. События, регистрируемые в журналах аудита. Защита объектов Windows с помощью дескриптора безопасности SECURITY_DESCRIPTOR (инициализация, определение SID владельца объекта, инициализация ACL, создание списков DACL и SACL, связывание списков с дескриптором безопасности, используемые для этого вызовы).	
1.6	Сетевые средства системы безопасности.	Элементы настройки и конфигурирования системы безопасности. Модули системы безопасности. Назначение локальной системы безопасности (LSA - local security authority), монитора безопасности (SRM - security reference monitor) и диспетчера безопасности (SAM - security account manager) в системе безопасности W. Аутентификация (нижний, средний и верхний уровни) Windows. Аудит в W. Журналы: системный, безопасности, приложений. IP безопасность (IPsec) - секретная связь открытых сетей нижнего уровня. Назначение, основные компоненты, политика соединений, IP - фильтры, агенты безопасности, протоколы сетевой защиты, алгоритмы шифрования. Сетевые технологии защиты SHTTP и SSL/TLS. Схема организации защищенной связи. Сравнение с IP безопасностью. Средства защиты IIS. Аутентификация в IIS (анонимный доступ, базовая, дайджест (хэш), интегрированная). Аутентификация на основе системы цифровой сертификации. Понятие о цифровом сертификате и системе сертификации. Сертифицирующие органы и доверенные центры. Состав информации сертификата. Система сертификации в W. Назначение модуля посредника, исполнительного модуля, модуля политики сертификации, выходного модуля. Организация иерархической системы сертификации. Примеры шаблонов сертификатов. Аутентификация на основе электронной цифровой подписи. Методы шифрования. Алгоритм Диффи - Хелмана. Аутентификация подлинности фирменных программ. Схема обмена данными Kerberos - клиента и Kerberos - сервера при доступе к удаленному ресурсному серверу. Алгоритмы первичной аутентификации и получения билета на доступ к удаленному серверу. Служба распределения ключей и выдачи билетов на сеансы связи в Kerberos. Аутентификация разных доменов и ее делегирование в Kerberos. Назначение и архитектура системы аутентификации SESAME. Назначение серверов	

		аутентификации, атрибутов привилегий и распределения ключей. Компоненты клиента и сервера.	
2. Лабораторные работы			
2.1	Лабораторная работа 1.	Программирование виртуального контроллера записи и чтения данных FLASH памяти, подключенного к одному из интерфейсов материнской платы.	Б1.В.ДВ.04.02 Безопасность системного программного обеспечения (10.05.01) https://edu.vsu.ru/course/
2.2	Лабораторная работа 2	Реализация задания лабораторной работы 2 с разработкой библиотеки модулей dll (3 - 5 модулей), выполняющих отдельные, по выбору студентов, операции процессов записи и чтения.	
2.3	Лабораторная работа 3	Разработка клиент - серверной программы.	
2.4	Лабораторная работа 4	Разработать клиент - серверную программу со следующими характеристиками: 1. Программа должна включать сервер и три - четыре клиента. 2. Сервер выполняет регистрацию клиентов, ввод логина, паролей и IP - адресов, сохраняя идентификационные данные в базе данных. Пароль вводится скрытно, подтверждается и хранится в незашифрованном виде. 3. После регистрации любой клиент может обмениваться данными с другими клиентами через сервер. Сервер после идентификации зарегистрированного клиента и наличии в базе данных запрашиваемого клиента предоставляет возможность обмена данными. В противном случае клиенту выдается отказ с объяснением причин отказа.	
2.5	Лабораторная работа 5	Разработать клиент - серверную программу со следующими характеристиками: 1. Программа должна включать сервер и три - четыре клиента. 2. Сервер выполняет регистрацию клиентов, ввод логина, паролей и IP - адресов, сохраняя идентификационные данные в базе данных, управляемой СУБД. 3. После регистрации любой клиент может обмениваться данными с другими клиентами через сервер. Сервер после идентификации зарегистрированного клиента и наличии в базе данных запрашиваемого клиента предоставляет возможность обмена данными. В противном случае клиенту выдается отказ с объяснением причин отказа. Незарегистрированному клиенту предоставляется возможность пройти процедуру регистрации. Для работы с базой данных использовать СУБД с применением SQL - запросов. Пароли хранить в зашифрованном виде. Допустимы простые алгоритмы шифрования.	
2.6	Лабораторная работа 6	Подсистемы безопасности в современных системах.	

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)					
		Лекции	Практ.	Лаб. раб.	Самостоятельная работа	Контроль	Всего
1.1	Системное программное обеспечение. Классификация системных программ.	4		4	10	0	18
1.2	Особенности выполнения программ. Синхронизация потоков. Решение классических проблем синхронизации и реализация синхронизации	4		6	10	0	20
1.3	Ввод-вывод. Принципы работы, программные уровни вводы-вывода.	6		6	10	0	22

	Драйвера устройств						
1.4	Подсистема безопасности	6		4	12	0	22
1.5	Информационная безопасность в операционных системах и сетях.	8		8	14	0	30
1.6	Сетевые средства системы безопасности.	8		8	16	0	32
	Итого:	36		36	72	0	144

14. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины включает в себя лекционные занятия, лабораторные занятия и самостоятельную работу обучающихся. На первом занятии студент получает информацию для доступа к комплексу учебно-методических материалов.

Лекционные занятия посвящены рассмотрению теоретических основ дисциплины. Лабораторные занятия предназначены для формирования умений и навыков, закрепленных компетенциями по ОПОП. Самостоятельная работа студентов включает в себя проработку учебного материала лекций, разбор лабораторных заданий, подготовку к экзамену.

Для успешного освоения дисциплины рекомендуется подробно конспектировать лекционный материал, просматривать презентации (при наличии) по соответствующей теме, изучать основную и дополнительную литературу рекомендуемой библиографии,

При использовании дистанционных образовательных технологий и электронного обучения выполнять все указания преподавателей по работе на LMS-платформе, своевременно подключаться к online-занятиям, соблюдать рекомендации по организации самостоятельной работы.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

а) основная литература:

№ п/п	Источник
1	Кручинин, В. В. Разработка сетевых приложений : учебное пособие / В. В. Кручинин. — Москва : ТУСУР, 2013. — 120 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/110372. — Режим доступа: для авториз. пользователей.
2	Форшоу, Д. Атака сетей на уровне протоколов / Д. Форшоу ; перевод с английского Д. А. Беликова. — Москва : ДМК Пресс, 2022. — 340 с. — ISBN 978-5-97060-972-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/241175. — Режим доступа: для авториз. пользователей.

б) дополнительная литература:

№ п/п	Источник
3	Ружников, В. А. Основы сетевого программирования на языке высокого уровня Python : учебно-методическое пособие / В. А. Ружников, М. А. Вержаковская. — Самара : ПГУТИ, 2019. — 136 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223331. — Режим доступа: для авториз. пользователей.
4	Шмытинский, В. В. Разработка системы тактовой сетевой синхронизации первичной сети связи : учебное пособие / В. В. Шмытинский, В. П. Глушко. — Санкт-Петербург : ПГУПС, 2021. — 39 с. — ISBN 978-5-7641-1612-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/191024. — Режим доступа: для авториз. пользователей.
5	Управление ИТ-инфраструктурой предприятия (архитектурный подход) : учебное пособие / Л. И. Зинина, Е. А. Сысоева, Л. И. Ефремова, А. В. Катынь. — Саранск : МГУ им. Н.П. Огарева, 2020. — 196 с. — ISBN 978-5-7103-3991-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/204689. — Режим доступа: для авториз. пользователей.

в) информационные электронно-образовательные ресурсы**:**

№ п/п	Источник
6	Электронно-библиотечная система «Лань» - Режим доступа: https://e.lanbook.com
7	Электронный каталог Научной библиотеки Воронежского государственного университета. - Режим доступа: http//:www.lib.vsu.ru.
8	Криптографические протоколы (10.05.01)/Степанец Ю.А. - Образовательный портал «Электронный университет ВГУ». — Режим доступа: https://edu.vsu.ru

16. Перечень учебно-методического обеспечения для самостоятельной работы

В качестве формы организации самостоятельной работы применяются

методические указания для самостоятельного освоения и приобретения навыков работы со специализированным программным обеспечением. Самостоятельная работа студентов: изучение теоретического материала; подготовка к лекциям, работа с учебно-методической литературой, подготовка отчётов по лабораторным работам, подготовка к экзамену.

Для обеспечения самостоятельной работы студентов в электронном курсе дисциплины на образовательном портале «Электронный университет ВГУ» сформирован учебно-методический комплекс, который включает в себя: программу курса, учебные пособия и справочные материалы, методические указания по выполнению заданий лабораторных работ. Студенты получают доступ к данным материалам на первом занятии по дисциплине.

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение)

Дисциплина реализуется с применением электронного обучения и дистанционных образовательных технологий. Для организации занятий рекомендован онлайн-курс «Б1.В.ДВ.04.02 Безопасность системного программного обеспечения (10.05.01)», размещенный на платформе Электронного университета ВГУ (LMS moodle), а также Интернет-ресурсы, приведенные в п.15в.5.

18. Материально-техническое обеспечение дисциплины

Учебная аудитория для лекций: специализированная мебель, компьютер преподавателя, мультимедийный проектор, экран.

Учебная аудитория для лабораторных занятий: специализированная мебель, персональные компьютеры, мультимедийный проектор, экран, лабораторное оборудование программно-аппаратных средств обеспечения информационной безопасности.

Аудитория для самостоятельной работы: учебная мебель, компьютер с возможностью подключения к сети «Интернет» и электронной платформе Электронного университета ВГУ.

Программное обеспечение (см.файл МТО): ОС Windows v.7, 8, 10, набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader.

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

ПК-1. Способен проводить анализ требований и выполнять работы по проектированию программных и аппаратных компонент системы безопасности компьютерных систем и сетей, в том числе с использованием современных методов и средств защиты информации

– ПК-1.1. применяет современные методы разработки программного обеспечения и технологии программирования

– ПК-1.3. использует принципы комплексной разработки правил, процедур, приемов и методов, при создании средств защиты информации, в том числе с использованием современных методов и средств разработки программного обеспечения

ПК-2. Способен принимать участие в экспертизе и анализе уязвимостей, угроз и инцидентов информационной безопасности в компьютерных системах и сетях

– ПК-2.1. применяет эффективные методы и средства планирования и организации исследований и разработки

ПК-3. Способен участвовать в работах по проектированию систем защиты информации в компьютерных системах и сетях при решении профессиональных, исследовательских и прикладных задач

– ПК-3.5. выполняет проверку устойчивости приложений к внешнему несанкционированному доступу, в том числе проверка устойчивости веб-приложений к атакам, применение средств контроля безопасности, управление криптографическими средствами, а также организация мероприятий по обеспечению кибербезопасности

№ п/п	Наименования раздела дисциплины	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1	Системное программное обеспечение. Классификация системных программ.	ПК-2	ПК-2.1	устный опрос, тест, лабораторная работа
2	Особенности выполнения программ. Синхронизация потоков. Решение классических проблем синхронизации и реализация синхронизации	ПК-1	ПК-1.1	устный опрос, тест, лабораторная работа
		ПК-2	ПК-2.1	устный опрос, тест, лабораторная работа
		ПК-3	ПК-3.5	устный опрос, тест, лабораторная работа
3	Ввод-вывод. Принципы работы, программные уровни вводы-вывода. Драйвера устройств	ПК-1	ПК-1.1	устный опрос, тест, лабораторная работа
		ПК-2	ПК-2.1	устный опрос, тест, лабораторная работа
4	Подсистема безопасности	ПК-1	ПК-1.1	устный опрос, тест, лабораторная работа
			ПК-1.3	устный опрос, тест, лабораторная работа
		ПК-2	ПК-2.1	устный опрос, тест, лабораторная работа
		ПК-3	ПК-3.5	устный опрос, тест, лабораторная работа
5	Информационная безопасность в операционных системах и сетях.	ПК-1	ПК-1.1	устный опрос, тест, лабораторная работа
			ПК-1.3	устный опрос, тест, лабораторная работа
		ПК-3	ПК-3.5	устный опрос, тест, лабораторная работа
6	Сетевые средства системы безопасности.	ПК-1	ПК-1.1	устный опрос, тест, лабораторная работа
			ПК-1.3	устный опрос, тест, лабораторная работа
		ПК-3	ПК-3.5	устный опрос, тест, лабораторная работа
Промежуточная аттестация, форма контроля - зачет с оценкой				Перечень вопросов (КИМ№1)

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

- лабораторные работы.

Перечень лабораторных работ

1	Лабораторная работа 1.	Программирование виртуального контроллера записи и чтения данных FLASH памяти, подключенного к одному из интерфейсов материнской платы.
2	Лабораторная работа 2	Реализация задания лабораторной работы 2 с разработкой библиотеки модулей dll (3 - 5 модулей), выполняющих отдельные, по выбору студентов, операции процессов записи и чтения.
3	Лабораторная работа 3	Разработка клиент - серверной программы.

4	Лабораторная работа 4	Разработать клиент - серверную программу со следующими характеристиками: 1. Программа должна включать сервер и три - четыре клиента. 2. Сервер выполняет регистрацию клиентов, ввод логина, паролей и IP - адресов, сохраняя идентификационные данные в базе данных. Пароль вводится скрытно, подтверждается и хранится в незашифрованном виде. 3. После регистрации любой клиент может обмениваться данными с другими клиентами через сервер. Сервер после идентификации зарегистрированного клиента и наличии в базе данных запрашиваемого клиента предоставляет возможность обмена данными. В противном случае клиенту выдается отказ с объяснением причин отказа.
5	Лабораторная работа 5	Разработать клиент - серверную программу со следующими характеристиками: 1. Программа должна включать сервер и три - четыре клиента. 2. Сервер выполняет регистрацию клиентов, ввод логина, паролей и IP - адресов, сохраняя идентификационные данные в базе данных, управляемой СУБД. 3. После регистрации любой клиент может обмениваться данными с другими клиентами через сервер. Сервер после идентификации зарегистрированного клиента и наличии в базе данных запрашиваемого клиента предоставляет возможность обмена данными. В противном случае клиенту выдается отказ с объяснением причин отказа. Незарегистрированному клиенту предоставляется возможность пройти процедуру регистрации. Для работы с базой данных использовать СУБД с применением SQL - запросов. Пароли хранить в зашифрованном виде. Допустимы простые алгоритмы шифрования.
6	Лабораторная работа 6	Подсистемы безопасности в современных системах.

Технология проведения
Все лабораторные работы обязательны для выполнение. Задание является общим для всех, выполняется индивидуально под наблюдением преподавателя.

Критерии оценивания

- оценивается «зачтено», если работа выполнена в полном объеме (приведены все задания, и они правильные, даны пояснения);

оценивается «не зачтено», работа выполнена не полностью или в представленной части много ошибок

20.2 Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств: вопросы к экзамену.

Перечень вопросов к экзамену (КИМ №1)

1. Верификация и тестирование программ. Особенности и отличия.
2. Метод математической индукции. Модифицированная, нисходящая и восходящая индукция.
3. Инвариант цикла и особенности его доказательства.
4. Метод индуктивных утверждений Флойда.
5. Запутывающие преобразования программного обеспечения, цели и задачи.
6. Методы запутывающих преобразований.
7. Формат команды процессора.
8. Структура исполняемого PE модуля.
9. Дизассемблирование. Цели и задачи. Примеры дизассемблеров и их характеристики.
10. Язык Ассемблера, коды и мнемонические имена. Примеры команд условного и безусловного перехода, пересылки данных, арифметических операций и операции сравнения. Принципы работы этих команд.

11. Преобразований потока управления для обфускации программ.
12. Лексическая обфускация, цели, задачи и примеры.
13. Преобразования форматирования для обфускации программ.
14. Жизненный цикл программного обеспечения.
15. Ролевой состав разработчиков программного обеспечения.
16. Модели жизненного цикла разработки программного обеспечения.
17. Привести фрагмент программы, содержащей "мертвый" и "избыточный" код.
18. Привести фрагмент программы, содержащей "недостижимый" код и "развертку" цикла.
19. Стандарты и классы защиты информации.
20. Локальные системы защиты в сетях.
21. Брандмауэры, их назначение и типы.
22. Характеристики фильтров пакетов, шлюзов прикладного уровня, шлюзов уровня каналов, и брандмауэров проверки пакетов с фиксацией состояния.
23. Криптографические интерфейсы.
24. Основные функции CryptAPI.
25. Система безопасности файловой системы EFS – encrypting file system.
26. Компьютерные вирусы.
27. Классификация компьютерных вирусов по среде обитания, по способу заражения среды обитания, по деструктивным возможностям, по особенностям алгоритмов заражения.
28. Файловые, загрузочные и макро вирусы.
29. Способы заражения командных и исполняемых и загружаемых драйверов. Алгоритмы работы загрузочных вирусов.
30. Уровни уязвимости различных операционных систем.
31. Методы борьбы с вирусами.
32. Методы обнаружения вирусов.
33. Аппаратная защита от вирусов.
34. Информационная безопасность в операционных системах и сетях.
35. Основные понятия безопасности информации. Каналы утечки. Объекты защиты. Возможные угрозы. Классификация угроз. Программные и аппаратные средства защиты информации.
36. Базовые принципы организации защиты.
37. Системный подход к организации защиты информации в компьютерных системах.
38. Общие правила защиты.
39. Безопасность в операционных системах. Типовая архитектура подсистемы защиты в операционных системах.
40. Разграничение доступа к объектам ОС.
41. Идентификация, аутентификация и авторизация субъектов доступа.
42. Организация парольных систем (требования при выборе, хранение, передача по сети, методы подбора, защита от компрометации).
43. Административные принципы защиты. Управление политиками безопасности.
44. Организация защиты информации в Windows.
45. Субъекты и объекты доступа (защиты).
46. Понятия о правах и привилегиях.
47. Комплексная система организации безопасности информации.
48. Организация защиты информации в Unix.
49. Стандарты и классы защиты информации.
50. Защита объектов Windows с помощью дескриптора безопасности SECURITY_DESCRIPTOR (инициализация, определение SID владельца объекта, инициализация ACL, создание списков DACL и SACL, связывание списков с дескриптором безопасности, используемые для этого вызовы).
51. Аудит. Требования к аудиту. Политика аудита. События, регистрируемые в журналах аудита.
52. Сетевые средства системы безопасности.
53. Сетевые средства системы безопасности W.
54. Элементы настройки и конфигурирования системы безопасности.
55. Модули системы безопасности.

56. Назначение локальной системы безопасности (LSA – local security authority), монитора безопасности (SRM – security reference monitor) и диспетчера безопасности (SAM – security account manager) в системе безопасности W.
57. Аутентификация (нижний, средний и верхний уровни) Windows.
58. Аудит в W. Журналы: системный, безопасности, приложений.
59. IP безопасность (IPsec) - секретная связь открытых сетей нижнего уровня.
60. Назначение, основные компоненты, политика соединений, IP – фильтры, агенты безопасности, протоколы сетевой защиты, алгоритмы шифрования.
61. Сетевые технологии защиты SHTTP и SSL/TLS. Схема организации защищенной связи.
62. Сравнение с IP безопасностью.
63. Средства защиты IIS. Аутентификация в IIS (анонимный доступ, базовая, дайджест (хэш), интегрированная).
64. Аутентификация на основе системы цифровой сертификации.
65. Понятие о цифровом сертификате и системе сертификации.
66. Сертифицирующие органы и доверенные центры.
67. Состав информации сертификата.
68. Система сертификации в W. Назначение модуля посредника, исполнительного модуля, модуля политики сертификации, выходного модуля. Организация иерархической системы сертификации. Примеры шаблонов сертификатов.
69. Аутентификация на основе электронной цифровой подписи.
70. Аутентификация подлинности фирменных программ.
71. Архитектура системы сетевой аутентификации Kerberos.
72. Схема обмена данными Kerberos - клиента и Kerberos – сервера при доступе к удаленному ресурсному серверу.
73. Алгоритмы первичной аутентификации и получения билета на доступ к удаленному серверу.
74. Служба распределения ключей и выдачи билетов на сеансы связи в Kerberos.
75. Аутентификация разных доменов и ее делегирование в Kerberos.
76. Назначение и архитектура системы аутентификации SESAME.
77. Назначение серверов аутентификации, атрибутов привилегий и распределения ключей.
78. Компоненты клиента и сервера.
79. Логическая организация ресурсов сетей. Доменная структура. Доверенные отношения между доменами. 4 модели доменов.
80. Служба Active Directory (AD) и ее назначение.
81. Дополнительные возможности системы безопасности и доменной системы сетей при работе с AD.
82. Особенности службы DNS (domain name service) в AD.
83. Базовые концепции архитектуры AD.
84. Назначение схемы каталогов (directory scheme), менеджера схемы каталогов (schema manager), глобального каталога (global catalog).
85. Виды делегирования административных полномочий в AD.
86. Интерфейс ADSI.
87. Поддержка доверительных отношений и делегирования аутентификации.
88. Варианты делегирования.
89. Локальные системы защиты в сетях.
90. Брандмауэры, их назначение и типы.
91. Характеристики фильтров пакетов, шлюзов прикладного уровня, шлюзов уровня каналов, и брандмауэров проверки пакетов с фиксацией состояния.
92. Криптографические интерфейсы. Основные функции CryptAPI.
93. Система безопасности файловой системы EFS – encrypting file system.
94. Формальные языки. Базовые понятия. Способы задания.
95. Трансляторы. Компиляторы и интерпретаторы.
96. Классы грамматик по Хомскому. Их характеристики и формальное задание.
97. Выводы цепочек. Конечно- автоматные языки, распознаватели и преобразователи.
98. Структура трансляторов формализованных языков.

99. Лексический, синтаксический и семантический анализаторы

Критерии оценки ответов на вопросы экзамена

Для оценивания результатов обучения на экзамене используется - 4-балльная шала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно», критерии оценивания приведены ниже.

Оценка «отлично» - студент демонстрирует глубокое понимание темы, умеет распространять вытекающие из теории выводы.
Оценка «хорошо» - студент демонстрирует понимание теоретических положений темы и базовых понятий, но допускает неточности в ответах, испытывает затруднения в применении знаний к анализу состояния проекта.
Оценка «удовлетворительно» - студент отвечает не на все предложенные вопросы, но не менее, чем на половину из них; не демонстрирует способности применения теоретических знаний для анализа ситуаций.
Оценка «неудовлетворительно» - студент демонстрирует непонимание теоретических основ и базовых понятий курса.

Оценка промежуточной аттестации формируется как интегральная оценка по следующей формуле (При округлении оценки используется правило правильного округления. При получении оценки не менее 3 баллов, выставляется «зачтено», менее 3 баллов - «не зачтено». При этом, все лабораторные работы должны быть выполнены и защищены

$$Q_{пром\_ат} = 0{,}2Q_{КР1} + 0{,}2Q_{КР2} + 0{,}6Q_{экз}$$

При округлении оценки используется правило правильного округления. При получении оценки не менее 3 баллов, выставляется «зачтено», менее 3 баллов - «не зачтено». При этом, все лабораторные работы должны быть выполнены и защищены.

20.3 Фонд оценочных средств сформированности компетенций студентов, рекомендуемый для проведения диагностических работ

ПК-1. Способен проводить анализ требований и выполнять работы по проектированию программных и аппаратных компонент системы безопасности компьютерных систем и сетей, в том числе с использованием современных методов и средств защиты информации;
ПК-2. Способен принимать участие в экспертизе и анализе уязвимостей, угроз и инцидентов информационной безопасности в компьютерных системах и сетях
ПК-3. Способен участвовать в работах по проектированию систем защиты информации в компьютерных системах и сетях при решении профессиональных, исследовательских и прикладных задач

1) закрытые задания (тестовые, средний уровень сложности):

1. Язык, в котором представлены команды процессора в более удобной для человека символьной форме записи, называется …
языком высокого уровня
объектно-ориентированным языком
машинным языком
проблемно-ориентированным языком
языком ассемблера
2. Преобразования, изменяющие иерархию наследования классов программы, относятся к группе…
преобразований потока управления
преобразования форматирования
общих преобразований
командных преобразований

преобразований структур данных
3. Преобразования исходного кода программы, которые переименовывают идентификаторы относятся к группе…
преобразований структур данных
преобразований потока управления
общих преобразований
командных преобразований
преобразований форматирования
4. Код программы, который выполняется, но его выполнение никак не влияет на результат работы программы, называется …
ненужным
лишним
избыточным
недостижимым
мертвым
5. Код программы, который выполняется и результат его выполнения используется в дальнейшем в программе, но такой код можно упростить или совсем удалить, называется …
ненужным
лишним
мертвым
недостижимым
избыточным
6. Приведение исполняемого кода к виду, сохраняющему функциональность программы, но затрудняющему анализ и понимание алгоритмов работы, называется …
дизассемблированием
валидацией
верификацией
аутентификацией
обфускацией

1. Совокупность итерационных процедур, связанных с последовательным изменением состояния программного обеспечения от формирования исходных требований к нему до окончания его эксплуатации конечным пользователем.
разработка программного обеспечения
написание исходного кода
внедрение программного обеспечения
верификация программного обеспечения
жизненный цикл программного обеспечения
2. В какой модели жизненного цикла разработки программного обеспечения на каждом эта-пе происходит реализация и тестирование одной функции системы, после завершения которых система сразу передается заказчику на проверку или эксплуатацию.
каскадный жизненный цикл
спиральный жизненный цикл
V-образный жизненный цикл
экстремальное программирование
3. В какой модели жизненного цикла разработки программного обеспечения переход к следующему этапу происходит только тогда, когда полностью завершены все работы предыдущего этапа.
экстремальное программирование
спиральный жизненный цикл
V-образный жизненный цикл
каскадный жизненный цикл
4. Кто из ролевого состава разработчиков программного обеспечения управляет коммуникациями и взаимоотношениями в проектной группе.
Разработчик
Специалист по тестированию

Специалист по контролю качества
Специалист по сертификации
Специалист по внедрению и сопровождению
Менеджер программы
5. Кто из ролевого состава разработчиков программного обеспечения участвует в анализе особенностей площадки заказчика, на которой планируется проводить внедрение разрабатываемой системы.
Разработчик
Специалист по тестированию
Специалист по контролю качества
Специалист по сертификации
Менеджер программы
Специалист по внедрению и сопровождению__

1. Что, по мнению Э. Дейкстры, может использоваться для демонстрации наличия ошибок в программном обеспечении, но никогда не покажет их отсутствие?
верификация
валидация
внедрение
сопровождение
тестирование
2. Формальное доказательство правильности работы программы это…
тестирование
валидация
внедрение
сопровождение
верификация
3. Условие, истинное перед выполнением программы называется…
инвариантом цикла
постусловием
условием завершения
условие правильной работы программы
предусловием
4. Для доказательства каких условий применятся метод математической индукции в верификации программ?
предусловия
постусловия
условия завершения
условия правильной работы программы
инварианта цикла
5. A – свойство переменных до выполнения программы (предусловие). C – свойство переменных после выполнения (постусловие). Если при каждом выполнении программы с данными, удовлетворяющими A, будет справедливо C, при условии, что программа закончится, то программа называется …
полностью правильной
наполовину правильной
частично неправильной
наполовину неправильной
частично правильной
6. Метод индуктивных утверждений позволяет доказать, что программа …
полностью правильна
наполовину правильна
частично неправильна
наполовину неправильна
частично правильна
7. В каких местах блок-схемы помимо пред- и постусловий, по крайней мере, должны быть

установлены условия согласно методу индуктивных утверждений?
в начале программы
в конце программы
перед условными операторами
нигде
перед входами в циклы
8. Условие, которое истинно перед началом выполнения цикла и не меняет своей истинности, в зависимости от числа итераций, называется …
постусловием
предусловием
условием завершения
условие правильной работы программы
инвариантом цикла
1. Дизассемблер позволяет …
написать и откомпилировать программу на языке ассемблера
сформировать исполняемый модуль
перевести программу с языка ассемблера на язык высокого уровня
откомпилировать программу
представить исполняемый модуль в виде команд на языке ассемблера
2. Выберите программы дизассемблеры.
Visual Studio
Rational Unified Process
DELPHI
Ida PRO
W32Dasm
3. Что содержит таблица импорта исполняемого PE-модуля?
информацию о структуре файла
машинные команды
информацию о ресурсах файла
информацию о функциях из динамически загружаемых библиотек
4. Информация о каких объекта хранится в блоке ресурсов исполняемого PE-модуля?
о динамических функциях
о директории модуля
о типе модуля
о курсоре мыши
о диалоговых окнах
5. Информация о каких объекта хранится в блоке ресурсов исполняемого PE-модуля?
о динамических функциях
о директории модуля
о типе модуля
о курсоре мыши
о диалоговых окнах
6. Команда пересылки на языке ассемблера.
add
jmp
sub
jne
mov
7. Команды условного и безусловного перехода на языке ассемблера.
add
mov
sub
jmp
jne

Задания раздела 20.3 рекомендуются к использованию при проведении

диагностических работ с целью оценки остаточных результатов освоения данной дисциплины (знаний, умений, навыков).