УТВЕРЖДЕНО
решением Ученого совета ФМИАТ
от «16» мая 2023 г., протокол № 4/23
Председатель _____ Волков М.А.
(подпись, расшифровка подписи)
«16» мая 2023 г.

РАБОЧАЯ ПРОГРАММА

Дисциплина	Защита программ и данных
Факультет	Математики, информационных и авиационных технологий
Кафедра	Информационной безопасности и теории управления
Курс	4

Специальность: 10.05.01 «Компьютерная безопасность»
код направления (специальности), полное наименование

Специализация: «Математические методы защиты информации»
полное наименование

Форма обучения: очная
очная, заочная, очно-заочная (указать только те, которые реализуются)

Дата введения в учебный процесс УлГУ: «01» 09 2023г.

Программа актуализирована на заседании кафедры: протокол №____ от _____ 20_____ г.
Программа актуализирована на заседании кафедры: протокол №____ от _____ 20_____ г.

Сведения о разработчиках:

ФИО	Кафедра	Должность, ученая степень, звание
Сутыркина Екатерина Алексеевна	ИБиТУ	доцент, к.ф-м.н

СОГЛАСОВАНО
Заведующий выпускающей кафедрой «Информационная безопасность и теория управления»
/_____/ Андреев А.С. / *(подпись)* *(Ф.И.О.)* «11» 05 2023г.

1. ЦЕЛИ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины:

- освоение студентом основных методов и средств анализа программных реализаций;
- организация защиты ПО от воздействий вредоносного характера и изучения третьими лицами;

Задачи освоения дисциплины:

- формирование навыков экспертизы качества и надежности реализаций программных средств обеспечения информационной безопасности;
- формирование навыков анализа программных реализаций на предмет наличия недокументированных возможностей;
- формирование навыков выявления вредоносного программного обеспечения и программных закладок;
- формирование навыков оценки опасности у обнаруженных вредоносных программ;
- развитие навыков организации антивирусной защиты;
- формирование навыков защиты информации на ПК и мобильных устройствах от изучения и модификации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к числу обязательных дисциплин специализации Б1.О и читается в 8-м семестре студентам специальности «Компьютерная безопасность» очной формы обучения.

Для успешного изучения дисциплины необходимы знания и умения, приобретенные в результате освоения курсов «Языки программирования», «Технологии и методы программирования», «Компьютерные сети», «Аппаратные средства вычислительной техники», «Защита в операционных системах».

Результаты освоения дисциплины будут необходимы для дальнейшего процесса обучения в рамках поэтапного формирования компетенций при изучении следующих дисциплин: «Компьютерные сети», «Основы построения защищенных компьютерных сетей», а также для научно-исследовательской работы и государственной итоговой аттестации.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СОТНЕСЕНЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины «Защита программ и данных» направлен на формирование следующих компетенций.

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
ОПК-13 Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности;	Знать: основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации Уметь: использовать средства защиты, проводить обоснование и выбор рационального решения по защите информационных систем с учетом заданных требований

	Владеть: принципами построения подсистем защиты информации и навыками разработки модели угроз и модели нарушителя безопасности компьютерных систем
ОПК-16 Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях;	Знать: способы, методы и критерии оценки эффективности реализации систем защиты информации. Уметь: применять отечественные и зарубежные стандарты для проектирования, разработки и оценивания защищенности компьютерной системы Владеть: приёмами, правилами проведению сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации.

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего) 3**.**

4.2. Объем дисциплины по видам учебной работы:

Вид учебной работы	Количество часов (форма обучения - дневная)			
	Всего по плану	В т.ч. по семестрам		
		8		
Контактная работа обучающихся с преподавателем	54	54		
Аудиторные занятия:				
•Лекции	36	36		
•Практические и семинарские занятия				
•Лабораторные работы (лабораторный практикум)	18	18		
Самостоятельная работа	54	54		
Форма текущего контроля знаний и контроля самостоятельной работы		Лабораторные работы, тестирование		
Курсовая работа				
Экзамен				
Всего часов по дисциплине	108	108		
Виды промежуточной аттестации (экзамен, зачет)		зачет		
Общая трудоемкость в зач. ед.	3	3		

4.3. Содержание дисциплины. Распределение часов по темам и видам учебной работы:

Форма обучения _____очная_____

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	
Раздел 1. Сети и анонимность							
1. Структура ОИС	5	2		1	*	2	лабораторная работа 1, тестирование
2. Протоколы и порты	4	2		0	*	2	тестирование
3.Анонимные сети	8	3		1	*	4	лабораторная работа 2, тестирование
4.Защиты переписки в сети.	5	2		1	*	2	лабораторная работа 3
Раздел 2. Вирусология							
5. ProВирусы	4	2		0	*	2	тестирование
6. Модель КС. Антивирусы	7	2		1	*	4	лабораторная работа 4, тестирование
7. Сэндбоксы	8	2		2	*	4	лабораторная работа 5, тестирование
8. Переполнение буфера. Дизассемблирование	9	2		1	*	6	лабораторная работа 6, тестирование
Раздел 3. Анализ кода и защита от анализа							
9. Тестирование кода: черный, серый, белый ящики	7	2		1	*	4	лабораторная работа 7, тестирование
10. Статический и динамический анализ кода	10	3		2	*	5	лабораторная работа 7, тестирование
11. Обфускация и деобфускация	5	2		1	*	2	лабораторная работа 8, тестирование
12. Шифрование	9	3		2	*	4	лабораторная работа 9, тестирование
13. Стеганография	7	2		1	*	4	лабораторная работа 10
Раздел 4. Безопасность данных							
14. Удаленный рабочий стол.	5	2		1	*	2	лабораторная работа 11, тестирование
15. Безопасность мобильных телефонов.	5	2		1	*	2	лабораторная работа 12
16. Форензика	10	3		2	*	5	лабораторная работа 13, тестирование
Зачет	2						
Итого	108	36		18	(18*)	54	

*-занятия проводятся в интерактивной форме

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Раздел 1. Сети и анонимность.

Тема 1. Структура ОИС. Эталонная модель OSI, модель TCP\IP, инкапсуляция, анализ содержимого пакетов на различных уровнях.

Тема 2. Протоколы и порты. Протоколы передачи данных в TCP\IP, распространенные службы и порты, на которых они работают, анализ запущенных приложений и выявление подозрительной активности процессов. Анализ сетевого трафика.

Тема 3. Анонимные сети. Способы анонимизации в сети. Ошибки, приводящие к деанонимизации. VPN, приватный режим, прокси, TOR.

Тема 4. Защиты переписки в сети. Способы отправки анонимных писем с помощью онлайн сервисов, защита переписки с помощью браузерных расширений и настройки почтовых клиентов.

Раздел 2. Вирусология.

Тема 5. Provирусы. Хронология эволюции компьютерных вирусов. Дополнительные требования к вирусу в условиях современной операционной системы. Стелс-механизмы в вирусах. Способы распространения вирусов. Сетевые вирусы. Основные классы современных сетевых вирусов. Алгоритмы функционирования вирусов. Методы получения доступа к ресурсам компьютеров-жертв.

Тема 6. Модель КС. Антивирусы. Формальные определения компьютерного вируса. Свойства компьютерного вируса. Общие сведения и базовые понятия формальной субъектно-ориентированной модели компьютерной системы. Наиболее известные формальные модели взаимодействия программной закладки с атакуемой системой. Дополнительные программные средства защиты компьютерной системы от программных закладок. Требования к дополнительным программным средствам защиты компьютерной системы от программных закладок.

Тема 7. Сэндбоксы. Классификация типичных схем взаимодействия программной закладки с атакуемой системой. Методы защиты компьютерных систем от программных закладок. Основные принципы компьютерной системы в отношении программных закладок. Принцип минимизации ПО. Принцип минимизации полномочий пользователя. Концепция изолированной программной среды. Сканирование системы на предмет наличия программных закладок. Сигнатурное сканирование. Эвристическое сканирование. Основные признаки наличия в сканируемом объекте компьютерного вируса. Способы “обмана” эвристического сканера. Достоинства и недостатки сигнатурного и эвристического сканирований.

Тема 8. Переполнение буфера. Дизассемблирование. Проблема Buffer overflow в реальной жизни, примеры и причины возникновения ошибки, способы избежать. Дизассемблеры и их условная классификация. Проблемы реализации алгоритмов дизассемблирования: проблема восстановления символических имен, проблема различения команд и данных, проблема определения границы машинной команды. Типовые особенности компиляции программ.

Раздел 3. Анализ кода и защита от анализа.

Тема 9. Тестирование кода: черный, серый, белый ящики. Описание метода экспериментов с черным, серым и белым ящиком. Варианты постановки задачи анализа программной реализации при применении метода экспериментов. Эффективность метода экспериментов. Недостатки метода экспериментов. Сведения об анализируемом программном продукте, получаемые методом экспериментов.

Тема 10. Статический и динамический анализ кода. Описание статического метода анализа программных реализаций. Эффективность статического метода. Описание динамического метода анализа программных реализаций. Отладка и отладчики. Факторы, ограничивающие возможности отладчика. Механизм работы отладчика. Флаги трассировки. Точки останова. Отладочные регистры и аппаратные точки останова. Достоинства и недостатки аппаратных точек останова. Метод маяков. Этапы анализа программы динамическим методом. Методы поиска интересующей функции. Метод маяков. Эффективность метода маяков. Выбор маяков. Пример применения метода маяков. Метод Step–Trace. Особенности применения метода Step-Trace. Эффективность метода Step-Trace. Метод анализа потоков внутри программы. Метод аппаратной точки останова. Эффективность метода аппаратной точки останова. Метод Step-Trace второго этапа. Методы анализа целевой функции программы. Пример применения динамического метода. Эффективность динамического метода.

Тема 11. Обфускация и деобфускация. Способы усложнения кода и защиты его от кодокопателей. Особенности функционирования обфусцированных программ, сервисы для обфускации и деобфускации кода.

Тема 12. Шифрование. Как зашифровать файлы, диск, флешку. Шифр Цезаря, шифрование с «солью», радужные таблицы, BASE64, RSA. Криптостойкость алгоритма RSA, возможность факторизации по открытому ключу.

Тема 13. Стеганография. Эволюция сокрытия информации на виду. Контейнеры и их основные признаки, ПО для стего-анализа.

Раздел 4. Безопасность данных.

Тема 14. Удаленный рабочий стол. Что такое RDP: как включить и как подключиться. Как настроить подключение к RDP из сети Интернет. Как подключиться к другому компьютеру и видеть его экран по RDP. RDP в Linux: запуск сервера и подключение к Windows. Аудит безопасности RDP. Брут-форс RDP. Сбор информации об RDP и через RDP.

Тема 15. Безопасность мобильных телефонов. Как защитить свой телефон от хакеров и кибератак. Антивирусы. Разрешения приложений. Антикриминалистика. Как защитить смартфон от извлечения данных.

Тема 16. Форензика. Форензика как наука о расследовании киберпреступлений. Классификация. Методы и техники экспертизы. Основные инструменты. Поиск артефактов. Анализ логов.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

Практические и семинарские занятия не предусмотрены учебным планом.

7. ЛАБОРАТОРНЫЕ РАБОТЫ (ЛАБОРАТОРНЫЙ ПРАКТИКУМ)

Лабораторная работа 1. Анализ трафика в сети.

Цель: анализ трафика, передаваемого по защищенному сетевому протоколу.

Содержание работы: разбор работы TLS, крипто-технологий, используемых для передачи данных, изучение информации о сертификате и удостоверяющем центре, подгрузка сохранённых в браузере ключей от сессий для анализа трафика в Wireshark.

Результат: отчёт от проделанной работе согласно руководству.

Лабораторная 2. Сравнение анонимных браузеров.

Цель: знакомство со свободно распространяемым ПО для веб-сёрфинга, выявление достоинств и недостатков анонимных браузеров.

Содержание работы: протестировать предложенные браузеры на уникальность отпечатков, составить сравнительную таблицу.

Результат: отчет, содержащий сводную информацию о тестируемых продуктах, их сильных и слабых сторонах в анонимизации веб-сёрфинга.

Лабораторная 3. Защита переписки.

Цель: познакомится с браузерными решениями и почтовыми клиентами для корпоративной переписки.

Содержание работы: установка и настройка плагинов браузера, обеспечивающих шифрование с открытым ключом, а также почтового клиента.

Результат: письма в электронном почтовом ящике, доступные для чтения только пользователю, имеющему ключ.

Лабораторная 4. Сравнение популярных антивирусов.

Цель: знакомство со свободно распространяемым ПО для антивирусной защиты ПК.

Содержание работы: протестировать предложенные антивирусы на распознавание малвари из открытой базы.

Результат: таблица, содержащая информацию о тестируемых продуктах, их сильных и слабых сторонах в обеспечении антивирусной защиты.

Лабораторная 5. Анализ малвари.

Цель: знакомство с основными принципами написания вируса, распознавания его антивирусным ПО и сокрытия действий малвари от анализаторов.

Содержание работы: написать простейший вирус-локер, протестировать его в песочнице, протестировать на выбранном антивирусе.

Результат: отчет о проделанной работе.

Лабораторная 6. Реализация и разбор Buffer overflow.

Цель: ознакомление с принципами возникновения ошибки переполнения буфера, способами избежать ошибок такого рода, работа с ассемблером.

Содержание работы: написать программу, заведомо содержащую ошибку переполнения буфера, разобраться в работе стека, принципах простановки указателей и внедрения shell-кода.

Результат: программа, вызывающая calc.exe, что заведомо не предусмотрено её функционалом.

Лабораторная 7. Тестирование кода.

Цель: знакомство с принципами тестирования черного, белого и серого ящиков, динамический и статический анализ кода.

Содержание работы: по входным и выходным данным программы выяснить, что за функция реализована в коде.

Результат: аналитический вид функции.

Лабораторная 8. Обфускация и деобфускация кода.

Цель: ознакомление с сервисами и способами усложнения кода и его деобфускации.

Содержание работы: поиск флага на веб-ресурсе, код которого обфусцирован.

Результат: флаг заданного формата.

Лабораторная 9. Взлом формы.

Цель: научиться использовать полученные навыки по анализу, дешифровке и деобфускации кода в совокупности.

Содержание работы: поиск ключа, необходимого для авторизации на веб-сервисе, путём исследования кода ресурса.

Результат: код для авторизации.

Лабораторная 10. Стеганографический анализ файлов.

Цель: обучение стего-анализу.

Содержание работы: исследовать предоставленные графические и аудио файлы на наличие скрытой информации.

Результат: предоставление флага или зашифрованного сообщения.

Лабораторная 11. Настройка RDP.

Цель: знакомство с протоколом удалённого рабочего стола.

Содержание работы: настройка удаленного рабочего стола, аудит безопасности RDP.

Результат: настройка удаленного рабочего стола и подключение к удалённому рабочему столу.

Лабораторная 12. Защита данных от извлечения на iOS и Android.

Цель: ознакомиться со способами защиты персональной информации на мобильном устройстве.

Содержание работы: изменение настроек мобильного телефона для максимальной защиты от антикриминалистической экспертизы.

Результат: мобильное устройство, максимально защищенное от угрозы извлечения данных третьими лицами.

Лабораторная 13. Анализ log файла.

Цель: научиться читать логи.

Содержание работы: исследование .log файла web-ресурса, подвергшегося sql-атаке.

Результат: данные, которые удалось похитить атакующему.

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

Курсовые работы, контрольные работы, рефераты не предусмотрены учебным планом.

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ (ЗАЧЕТУ)

1. Эталонная модель OSI, модель TCP\IP.
2. Инкапсуляция, декапсуляция, анализ содержимого пакетов на различных уровнях.
3. Протоколы передачи данных в TCP\IP, распространенные службы и порты, на которых они работают.
4. Способы анализа запущенных приложений и выявление подозрительной активности процессов.
5. Способы анонимизации в сети. Ошибки, приводящие к деанонимизации.
6. Виртуальные частные сети, особенности, преимущества и недостатки.
7. Приватный режим в браузере, настройка, способы защитить данные веб-сёрфинга и возможность просочиться сквозь сеанс.
8. Разновидности прокси, TOR: служба и браузер.
9. Способы отправки анонимных писем с помощью онлайн сервисов.
10. Защита переписки с помощью браузерных расширений и настройки почтовых клиентов.
11. Хронология эволюции компьютерных вирусов. Основная классификация. Современные тенденции.
12. Дополнительные требования к вирусу в условиях современной операционной системы. Способы распространения вирусов. Методы получения доступа к ресурсам компьютеров-жертв.
13. Субъектно-ориентированная модель компьютерной системы. Формальные определения компьютерного вируса. Свойства компьютерного вируса.
14. Основные формальные модели взаимодействия программной закладки с атакуемой системой.
15. Достоинства, недостатки и принципы функционирования каждой формальной модели взаимодействия программной закладки и атакуемой системы: «наблюдатель», «перехват», «искажение», «уборка мусора».
16. Основные средства и методы защиты от программных закладок.
17. Основные организационные и административные меры антивирусной защиты.
18. Основные принципы компьютерной системы в отношении программных закладок. Принцип минимизации ПО. Принцип минимизации полномочий пользователя. Концепция изолированной программной среды.
19. Сканирование системы на предмет наличия программных закладок. Сигнатурное сканирование. Эвристическое сканирование.

20. Основные признаки наличия в сканируемом объекте компьютерного вируса. Способы “обмана” эвристического сканера. Достоинства и недостатки сигнатурного и эвристического сканирований.
21. Работа с дизассемблерами, их условная классификация.
22. Проблемы реализации алгоритмов дизассемблирования: проблема восстановления символических имен, проблема различения команд и данных, проблема определения границы машинной команды.
23. Постановка задачи анализа программных реализаций. Этапы анализа программных реализаций.
24. Метод экспериментов с черным, серым и белым ящиком.
25. Описание, возможности, достоинства и недостатки динамического метода анализа программных реализаций.
26. Описание, возможности, достоинства и недостатки статического метода анализа программных реализаций.
27. Основные методы поиска интересующей функции в программной реализации.
28. Метод маяков, метод Step-Trace, флаги, аппаратные точки останова.
29. Постановка задачи защиты программных реализаций от изучения. Достоинства и недостатки защиты программных реализаций от анализа
30. Основные способы защиты программных реализаций от анализа: динамическое изменение кода программы, искусственное усложнение структуры программы.
31. Распространённые алгоритмы шифрования, способы их распознать и дешифровка.
32. Шифрование с открытым ключом RSA. Возможность факторизации.
33. Основные принципы стеганографии. Области применения.
34. Основные признаки аудио и графических контейнеров. Способы внедрения и вычленения сокрытой информации.
35. Этапы настройки удалённого рабочего стола и способы обеспечения безопасного соединения и сохранности данных в течение сеанса.
36. Основные угрозы при использовании RDP и защита от них.
37. Повышение степени защиты данных, хранящихся на мобильном устройстве.
38. Форензика как наука о расследовании киберпреступлений. Методы и техники экспертизы.

10. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

Название разделов и тем	Вид самостоятельной работы	Объем в часах	Форма контроля
1. Структура ОИС	Проработка учебного материала, подготовка к сдаче зачета, лабораторные работы	2	лабораторная работа, тестирование, зачет
2. Протоколы и порты	Проработка учебного материала, подготовка к сдаче зачета	2	тестирование, зачет
3.Анонимные сети	Проработка учебного материала, подготовка к сдаче зачета, лабораторные работы	4	лабораторная работа, тестирование, зачет
4.Защиты переписки в сети.	Проработка учебного материала, подготовка к сдаче зачета, лабораторные работы	2	лабораторная работа, зачет
5. ProВирусы	Проработка учебного материала, подготовка к сдаче зачета	2	тестирование, зачет
6. Модель КС. Антивирусы	Проработка учебного материала, подготовка к сдаче зачета, лабораторные работы	4	лабораторная работа, тестирование, зачет
7. Сэндбоксы	Проработка учебного материала, подготовка к сдаче зачета, лабораторные работы	4	лабораторная работа, тестирование, зачет
8. Переполнение буфера. Дизассемблирование	Проработка учебного материала, подготовка к сдаче зачета, лабораторные работы	6	лабораторная работа, тестирование, зачет
9. Тестирование кода: черный, серый, белый ящики	Проработка учебного материала, подготовка к сдаче зачета, лабораторные работы	4	лабораторная работа, тестирование, зачет
10. Статический и динамический анализ кода	Проработка учебного материала, подготовка к сдаче зачета, лабораторные работы	5	лабораторная работа, тестирование, зачет
11. Обфускация и деобфускация	Проработка учебного материала, подготовка к сдаче зачета, лабораторные работы	2	лабораторная работа, тестирование, зачет
12. Шифрование	Проработка учебного материала, подготовка к сдаче зачета, лабораторные работы	4	лабораторная работа, тестирование, зачет
13. Стеганография	Проработка учебного материала, подготовка к сдаче зачета, лабораторные работы	4	лабораторная работа, зачет
14. Удаленный рабочий стол.	Проработка учебного материала, подготовка к сдаче зачета, лабораторные работы	2	лабораторная работа, тестирование, зачет
15. Безопасность мобильных телефонов.	Проработка учебного материала, подготовка к сдаче зачета, лабораторные работы	2	лабораторная работа, зачет
16. Форензика	Проработка учебного материала, подготовка к сдаче зачета, лабораторные работы	5	лабораторная работа, тестирование, зачет

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы

основная

1. *Казарин, О. В.* Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2023. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/513300 (дата обращения: 15.09.2023).

дополнительная

1. Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами / А. И. Белоус, В. А. Солодуха. - Москва : Инфра-Инженерия, 2020. - 692 с. - ISBN 978-5-9729-0486-0. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785972904860.html (дата обращения: 15.09.2023). - Режим доступа : по подписке.
2. Климентьев К.Е., Компьютерные вирусы и антивирусы: взгляд программиста / Климентьев К.Е. - М. : ДМК Пресс, 2013. - 656 с. - ISBN 978-5-94074-885-4 - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : http://www.studentlibrary.ru/book/ISBN9785940748854.html

Учебно-методическая

1. Сутыркина Е. А. Методические указания к лабораторным работам по дисциплине «Защита программ и данных» для студентов специальностей 10.05.01 «Компьютерная безопасность» и 10.05.03 «Информационная безопасность автоматизированных систем» очной формы обучения / Е. А. Сутыркина; УлГУ, Фак. математики, информ. и авиац. технологий. - Ульяновск : УлГУ, 2019. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 524 КБ). - Текст : электронный. http://lib.ulsu.ru/MegaPro/Download/MObject/5606

Согласовано:

Ведущий специалист НБ УлГУ	/ Терехина Л.А. /	_____	/ 10.05.2023 /
должность сотрудника научной библиотеки	ФИО	подпись	дата

б) Программное обеспечение

МойОфис Стандартный, Альт Рабочая станция 8.

Для образовательного процесса по данной дисциплине необходим стационарный класс ПК с установленным следующим программным обеспечением :

- Hex-Rays IDA Pro Disassembler,
- OllyDbg.
- Eclipse CDT
- Wireshark.

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1.1. Цифровой образовательный ресурс IPRsmart : электронно-библиотечная система : сайт / ООО Компания «Ай Пи Ар Медиа». - Саратов, [2023]. – URL: http://www.iprbookshop.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. Образовательная платформа ЮРАЙТ : образовательный ресурс, электронная библиотека : сайт / ООО Электронное издательство «ЮРАЙТ». – Москва, [2023]. - URL: https://urait.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. База данных «Электронная библиотека технического ВУЗа (ЭБС «Консультант студента») : электронно-библиотечная система : сайт / ООО «Политехресурс». – Москва, [2023]. – URL: https://www.studentlibrary.ru/cgi-bin/mb4x. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Консультант врача. Электронная медицинская библиотека : база данных : сайт / ООО «Высшая школа организации и управления здравоохранением-Комплексный медицинский консалтинг». – Москва, [2023]. – URL: https://www.rosmedlib.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО «Букап». – Томск, [2023]. – URL: https://www.books-up.ru/ru/library/ . – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.6. ЭБС Лань : электронно-библиотечная система : сайт / ООО ЭБС «Лань». – Санкт-Петербург, [2023]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. ЭБС Znanium.com : электронно-библиотечная система : сайт / ООО «Знаниум». - Москва, [2023]. - URL: http://znanium.com . – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. / ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2023].

3. Базы данных периодических изданий:

3.1. eLIBRARY.RU: научная электронная библиотека : сайт / ООО «Научная Электронная Библиотека». – Москва, [2023]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

3.2. Электронная библиотека «Издательского дома «Гребенников» (Grebinnikon) : электронная библиотека / ООО ИД «Гребенников». – Москва, [2023]. – URL: https://id2.action-media.ru/Personal/Products. – Режим доступа : для авториз. пользователей. – Текст : электронный.

4. Федеральная государственная информационная система «Национальная электронная библиотека» : электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2023]. – URL: https://нэб.рф. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. Российское образование : федеральный портал / учредитель ФГАУ «ФИЦТО». – URL: http://www.edu.ru. – Текст : электронный.

6. Электронная библиотечная система УлГУ : модуль «Электронная библиотека» АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: http://lib.ulsu.ru/MegaPro/Web. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

Согласовано:

Инженер ведущий	/ Щуренко Ю.В.	/	/ 04.05.2023
Должность сотрудника УИТТ	ФИО	подпись	дата

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Аудитория -3/316. Аудитория для проведения лекционных, семинарских и практических занятий, текущего контроля и промежуточной аттестации, групповых и индивидуальных консультаций. Комплект переносного мультимедийного оборудования: ноутбук с выходом в Интернет, экран, проектор, Wi-Fi с доступом в Интернет, ЭИОС,ЭБС. 432017, Ульяновская область, г. Ульяновск, ул. Набережная реки Свияги, д. 106-3 корпус.

Аудитория 24б для проведения лабораторных и практических занятий, текущего контроля и промежуточной аттестации, групповых и индивидуальных консультаций. 11 персональных компьютеров, проектор, экран, системы защиты информации: Соболь, Аккорд, Dallas Lock, Secret Net Studio. Сервер Vimark, АПКШ "Континент", Маршрутизаторы Cisco, Система защиты информации ViPNet. 432017, Ульяновская обл, г Ульяновск, ул Набережная реки Свияги, д 106-2 корпус.

Аудитория -230. Аудитория для самостоятельной работы. Аудитория укомплектована ученической мебелью. 16 персональных компьютеров.

Аудитория -237. Читальный зал научной библиотеки с зоной для самостоятельной работы. Аудитория укомплектована ученической мебелью. Компьютерная техника, телевизор, экран, проектор. Стол для лиц с ОВЗ. 432017, Ульяновская область, г. Ульяновск, р-н Железнодорожный, ул. Набережная р. Свияги, № 106-1 корпус.

Реализация программы дисциплины требует наличия учебной лаборатории. Оборудование учебной лаборатории: посадочные места по количеству студентов. Технические средства обучения: компьютеры с лицензионным программным обеспечением:

- Hex-Rays IDA Pro Disassembler,
- OllyDbg.
- Eclipse CDT
- Wireshark.

13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться некоторые из следующих вариантов восприятия информации с учетом их индивидуальных психофизических особенностей:

– для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации;

– для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации;

– для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий, организация работы ППС с обучающимися с ОВЗ и инвалидами предусматривается в электронной информационно-образовательной среде с учетом их индивидуальных психофизических особенностей.

Разработчик: _____ доцент _____ Сутыркина Екатерина Алексеевна
подпись должность ФИО