УТВЕРЖДЕНО

решением Ученого совета факультета математики,
информационных и авиационных технологий
от «21» 05 2024г., протокол № 5/24
Председатель _____ Волков М.А.
«21» 05 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	**Анализ уязвимостей программного обеспечения**
Факультет	Факультет математики, информационных и авиационных технологий
Кафедра	Кафедра информационной безопасности и теории управления
Курс	4 - очная форма обучения

Направление (специальность): 10.05.03 Информационная безопасность автоматизированных систем
Направленность (профиль/специализация): Безопасность открытых информационных систем Форма обучения: очная _____
Дата введения в учебный процесс УлГУ: 01.09.2024 г.
Программа актуализирована на заседании кафедры: протокол № 10 от 15.04.2024 г.
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	Кафедра информационной безопасности и теории управления	Доцент,Кандидат физико-математических наук

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины:

·освоение студентом основных методов и средств анализа программных реализаций;

·организация защиты ПО от воздействий вредоносного характера;

Задачи освоения дисциплины:

·формирование навыков экспертизы качества и надежности реализаций программных и программно-аппаратных 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 планирования работ по локализации последствий и пресечению обнаруженной атаки;

·развитие навыков организации антивирусной защиты;

·формирование навыков защиты программных реализации от изучения и модификации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Анализ уязвимостей программного обеспечения» относится к числу дисциплин блока Б1.В.1.ДВ.05, предназначенного для студентов, обучающихся по направлению: 10.05.03 Информационная безопасность автоматизированных систем.

В процессе изучения дисциплины формируются компетенции: ПК-3, ПК-6.

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: Подготовка к сдаче и сдача государственного экзамена, Подготовка к процедуре защиты и защита выпускной квалификационной работы, Защита программ и данных, Преддипломная практика, Функциональный анализ, Эксплуатационная практика, Теоретико-числовые методы и алгоритмы, информационные технологии в автоматизированных системах, Виртуальные частные сети, Сертификация средств защиты информации, Теория управления в информационных системах, Вейвлет-анализ, Системный анализ, Математические модели информационных систем, Методы принятия оптимальных решений, Нелинейные динамические системы, Модели безопасности компьютерных систем, Теория вычислительной сложности, Инструментальные средства контроля защищенности информации, Технические средства обнаружения каналов утечки информации,

Компьютерные сети, Аттестация объектов информатизации.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Код и наименование реализуемой компетенции	**Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций**
ПК-3 Способен разрабатывать проектные решения по защите информации в автоматизированных системах	**знать**: Критерии оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем **уметь**: Определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе **владеть**: Навыками разработки предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах
ПК-6 Способен проводить контроль защищенности информации от несанкционированного доступа	**знать**: Методы защиты информации и методики контроля защищенности информации от несанкционированного доступа и специальных программных воздействий на нее **уметь**: Проводить оценку защищенности информации от несанкционированного доступа и специальных воздействий Проверять работоспособность средств защиты информации от несанкционированного доступа и специальных воз-действий, выполнение правил их эксплуатации **владеть**: Навыками проведения контроля защищенности информации от несанкционированного доступа и специальных воздействий

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего): 3 ЗЕТ

4.2. Объем дисциплины по видам учебной работы (в часах): 108 часов

Форма обучения: очная

Вид учебной работы	**Количество часов (форма обучения очная)**	
	Всего по плану	**В т.ч. по семестрам**
		8
1	**2**	**3**
Контактная работа обучающихся с преподавателем в соответствии с УП	54	54
Аудиторные занятия:	54	54

Вид учебной работы	Количество часов (форма обучения очная)	
	Всего по плану	В т.ч. по семестрам
		8
1	2	3
Лекции	36	36
Семинары и практические занятия	-	-
Лабораторные работы, практикумы	18	18
Самостоятельная работа	54	54
Форма текущего контроля знаний и контроля самостоятельной работы: тестирование, контр. работа, коллоквиум, реферат и др. (не менее 2 видов)	Тестирование	Тестирование
Курсовая работа	-	-
Виды промежуточной аттестации (экзамен, зачет)	Зачёт	Зачёт
Всего часов по дисциплине	108	108

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	8
Раздел 1. Анализ программных реализаций							
Тема 1.1. Постановка задачи анализа программных реализаций.	9	1	0	4	0	4	Тестирование
Тема 1.2. Метод экспериментов с “черным	4	2	0	0	0	2	Тестирование

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	8
ящиком”.							
Тема 1.3. Статический метод.	4	2	0	0	0	2	Тестирование
Тема 1.4. Динамический метод.	4	2	0	0	0	2	Тестирование
Тема 1.5. Особенности анализа некоторых видов программ	6	2	0	0	0	4	Тестирование
Раздел 2. Защита программных реализаций							
Тема 2.1. Постановка задачи защиты программных реализаций от изучения	10	1	0	5	0	4	Тестирование
Тема 2.2. Динамическое изменение кода программы.	4	2	0	0	0	2	Тестирование
Тема 2.3. Искусственное усложнение структуры программы	4	2	0	0	0	2	Тестирование
Тема 2.4. Нестандартные обращения к	4	2	0	0	0	2	Тестирование

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	8
функциям операционной системы.							
Тема 2.5. Искусственное усложнение алгоритмов обработки данных	4	2	0	0	0	2	Тестирование
Тема 2.6. Выявление факта выполнения программы под отладчиком.	4	2	0	0	0	2	Тестирование
Раздел 3. Программные закладки, пути их внедрения, средства и методы противодействия программным закладкам							
Тема 3.1. Программные закладки и формальные модели их взаимодействия с атакуемой системой.	15	2	0	9	0	4	Тестирование
Тема 3.2. Формальная модель “наблюдатель”.	4	2	0	0	0	2	Тестирование
Тема 3.3. Формальная модель “перехват”.	4	2	0	0	0	2	Тестирование

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	8
Тема 3.4. Формальная модель “искажение”.	4	2	0	0	0	2	Тестирование
Тема 3.5. Методы внедрения программных закладок.	6	2	0	0	0	4	Тестирование
Тема 3.6. Компьютерные вирусы	6	2	0	0	0	4	Тестирование
Тема 3.7. Средства и методы защиты от программных закладок	6	2	0	0	0	4	Тестирование
Тема 3.8. Организационные и административные меры антивирусной защиты.	6	2	0	0	0	4	Тестирование
Итого подлежит изучению	108	36	0	18	0	54	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Анализ программных реализаций

Тема 1.1. Постановка задачи анализа программных реализаций.

Постановка задачи анализа программных реализаций. Актуальность задачи анализа программных реализаций. Этапы анализа программной реализации. Подходы к восстановлению алгоритмов, реализуемых программой.

Тема 1.2. Метод экспериментов с “черным ящиком”.

Описание метода экспериментов с “черным ящиком”. Варианты постановки задачи анализа программной реализации при применении метода экспериментов с “черным ящиком”. Эффективность метода экспериментов. Недостатки метода экспериментов. Сведения об анализируемом программном продукте, получаемые методом экспериментов: формат заголовков бинарного файла данных, наличие или отсутствие марканта в криптосистеме, зависимость марканта, используемого криптосистемой, от текущего времени, тип криптографического преобразования. Пример применения метода экспериментов.

Тема 1.3. Статический метод.

Описание статического метода анализа программных реализаций. Эффективность статического метода. 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. Дизассемблер IDA Pro и плагин Hex-Rays и их возможности. Пример применения статического метода.

Тема 1.4. Динамический метод.

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 1.5. Особенности анализа некоторых видов программ

Оверлейные программы. Проблемы анализа оверлейных программ. Диспетчер оверлеев. Проблемы анализа графических программ под Windows. Модификация метода Step-Trace. Использование Spy++. Проблемы анализа оконных функций программы и функций программы, вызываемых из них. Проблемы анализа диалоговых функций программ. Пример анализа графической программы в ОС семейства Windows. Проблемы анализа параллельного кода. Проблемы анализа кода в режиме ядра в ОС семейства Windows. Системные отладчики. Системный отладчик Syser. Особенности работы с отладчиком Syser. Вспомогательные инструменты анализа программ. Монитор активности процессов ProcMon. Возможности утилиты ProcMon. Утилита управления процессами Process Explorer. Возможности утилиты Process Explorer. Свойства процессов, определяемые утилитой Process Explorer.

Раздел 2. Защита программных реализаций

Тема 2.1. Постановка задачи защиты программных реализаций от изучения

Постановка задачи защиты программных реализаций от изучения Важность защиты программ от анализа. Причины отказа от приемов зашиты программных реализаций от анализа. Достоинства и недостатки защиты программных реализаций от анализа. Пример программы с защитой от анализа. Способы включения защиты от анализа в программную реализацию.

Тема 2.2. Динамическое изменение кода программы.

Способы организации динамического изменения кода программы. Понятие распаковщика. Распаковка кода. Распаковщик UPX. Преимущества и недостатки распаковщиков. Полиморфное преобразование кода. Наиболее простые полиморфные преобразования кода. «Засеивание» кода «пустышками». Вставка в код команд условных переходов на случайные адреса по тождественно ложным условиям. Замена команд синонимами. Замена регистров и (или) локальных переменных, используемых командами. Недостатки полиморфных преобразований.

Тема 2.3. Искусственное усложнение структуры программы

Способы искусственного усложнения структуры программы. Вызов функции нестандартными способами. Косвенный вызов функции. Вызов функции посредством машинной команды ret. Вызов функции через обработчик исключительной ситуации. Вызов функции в отдельном потоке. Вызов функции через пул потоков worker thread. Вызов функции через пул потоков wait thread. Вызов функции через передачу некоторому окну нестандартного сообщения. Вызов функции по таймеру. Вызов функции через перечисление дочерних окон окна, содержащего единственное дочернее окно. Вызов функции через перечисление главных окон программы, имеющей единственное главное окно. Вызов функции через перечисление файлов подкачки системы, имеющей единственный файл подкачки. Вызов функции через асинхронный ввод-вывод. Нестандартные способы сравнения данных.

Тема 2.4. Нестандартные обращения к функциям операционной системы.

Способы организации нестандартного обращения к функциям операционной системы. Динамический импорт. Использование более низкоуровневых системных функций, чем обычно. Использование собственных реализаций стандартных функций и компонент в ОС семейства Windows. Использование посреднического драйвера. Использование нестандартных путей реализации тех или иных системных функций. Модификация таблицы адресов импортов программы в ходе выполнения программы.

Тема 2.5. Искусственное усложнение алгоритмов обработки данных

Способы искусственного усложнения алгоритмов обработки данных. Многократное копирование данных с места на место. Копирование одних и тех же данных с использованием по назначению только одной из копий. Применение к данным сложных преобразований. Разбиение алгоритмов обработки данных на фрагменты. Усложненная обработка ошибок. Искусственное усложнение формата данных. Хранение данных в необычных местах.

Тема 2.6. Выявление факта выполнения программы под отладчиком.

Использование одного из процессов программной реализации в качестве отладчика. Использование программных ошибок конкретных отладчиков. Защита от анализа драйверов, выполняющихся в режиме ядра ОС семейства Windows. Перехват прерываний 1 и 3, используемых отладчиками. Анализ содержимого отладочных регистров в целях выявления аппаратных точек останова. Временное перенаправление стека текущего потока на область оперативной памяти, любое обращение к которой вызывает фатальную исключительную ситуацию.

Раздел 3. Программные закладки, пути их внедрения, средства и методы противодействия программным закладкам

Тема 3.1. Программные закладки и формальные модели их взаимодействия с атакуемой системой.

Общие сведения. Понятие программной закладки. Основная опасность программных закладок. Наиболее известные программные закладки. Общие сведения и базовые понятия формальной субъектно-ориентированной модели компьютерной системы. Наиболее известные формальные модели взаимодействия программной закладки с атакуемой системой. Классификация типичных схем взаимодействия программной закладки с атакуемой системой.

Тема 3.2. Формальная модель “наблюдатель”.

Описание формальной модели “наблюдатель”. Особенности, возможности и недостатки программных закладок класса “наблюдатель”. Скрытый удаленный контроль зараженной системы. Дополнительные задачи, решаемые программными закладками класса “наблюдатель”. Примеры программных закладок: Back Orifice, NetBus, Pinch. Клиент-серверная архитектура, требования к серверной части и обобщенная схема функционирования программной закладки класса “наблюдатель”. Маскировка протокола взаимодействия клиента и сервера программной закладки класса “наблюдатель”.

Тема 3.3. Формальная модель “перехват”.

Описание формальной модели “перехват”. Основные объекты перехвата. Способы перехвата паролей. Алгоритм работы перехватчика паролей первого рода. Алгоритм работы клавиатурного фильтра (перехватчика паролей второго рода). Алгоритм работы заместителя подсистемы аутентификации (перехватчика паролей третьего рода). Мониторы файловых систем. Монитор сети. Принципы работы монитора сети. Типы сетевых пакетов, подходящих для перехвата. Программная закладка класса “уборка мусора. Достоинства и недостатки программных закладок класса “перехват” каждого вида.

Тема 3.4. Формальная модель “искажение”.

Описание формальной модели “искажение”. Методы несанкционированного повышения полномочий пользователей. Несанкционированное использование средств динамического изменения полномочий. Примеры несанкционированного использования средств динамического

изменения полномочий в ОС семейства UNIX и Windows. Метод порождения дочернего процесса системным процессом и его техническая реализация. Метод модификации машинного кода монитора безопасности объектов. Вариации формальной модели “искажение”. Стелс-технологии. Стелс-драйвер. Функции стелс-драйвера.

Тема 3.5. Методы внедрения программных закладок.

Внедрение программной закладки в атакуемую систему в терминах субъектно-ориентированной модели. Классификация методов внедрения программных закладок. Метод маскировки программной закладки под прикладное ПО и его вариации. Пример реализации маскировки программной закладки под прикладное ПО. Маскировка программной закладки под системное ПО. Метод подмены системного ПО. Выбор программного модуля для подмены. Возможности реализации метода подмены системного программного обеспечения в современных ОС. Метод прямого ассоциирования программной закладки с программным модулем. Метод косвенного ассоциирования программной закладки с программным модулем. Особенности, достоинства и недостатки каждого из методов внедрения программных закладок.

Тема 3.6. Компьютерные вирусы

Формальные определения компьютерного вируса. Свойства компьютерного вируса. Краткая хронология эволюции компьютерных вирусов. Требования к компьютерному вирусу. Дополнительные требования к вирусу в условиях современной операционной системы. Стелс-механизмы в вирусах. Способы распространения вирусов. Сетевые вирусы. Краткая хронология развития сетевых вирусов. Вирус MSBlast, его возникновение и особенности. Основные классы современных сетевых вирусов. Онлайн-вирусы. Алгоритмы функционирования онлайн-вирусов. Методы получения доступа к ресурсам компьютеров-жертв. Почтовые вирусы. Отличия почтовых вирусов от онлайн-вирусов. Этапы работы почтового вируса: выбор очередной жертвы, заполнение темы и тела электронного письма, прикрепление вируса к письму, отправка зараженного письма жертве. Способы реализации этапов работы почтового вируса.

Тема 3.7. Средства и методы защиты от программных закладок

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. Дополнительные программные средства защиты компьютерной системы от программных закладок. Требования к дополнительным программным средствам защиты компьютерной системы от программных закладок. Методы борьбы с программными закладками в компьютерных системах. 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 3.8. Организационные и административные меры антивирусной защиты.

Основные мероприятия по организационному сопровождению антивирусной зашиты.

Инструктирование пользователей. Выбор момента проведения инструктажа пользователей. Просмотр и анализ данных регистрации и мониторинга. Контроль качества аутентификационных данных пользователей. Регулярные проверки адекватности поведения лиц, ответственных за обеспечение антивирусной защиты сети, в случае успешных вирусных атак. Регулярные инспекции состояния антивирусной защиты.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

7. ЛАБОРАТОРНЫЕ РАБОТЫ, ПРАКТИКУМЫ

Повторение. Основы работы с ассемблером.
Цели: повторение основных элементов языка ассемблера и соответствующих приемов работы с ассемблером.
Содержание: программа на языке ассемблера для процессоров Intel и ее структура, основные команды в языке ассемблера для процессоров Intel, прерывания, файловые операции в ОС Windows, ассемблерные макроопределения.
Результаты: консольное приложение, реализующее решение поставленной задачи.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/5603
Анализ программных реализаций.
Цели: получение навыков анализа программных реализаций, работы с отладчиками и дизассемблерами.
Содержание: анализ программных реализаций методом экспериментов с “черным ящиком” и его разновидности, статический метод анализа программных реализаций и его разновидности, динамический метод анализа программных реализаций и его разновидности, анализ оверлейных программ и оконных приложений в ОС семейства Windows.
Результаты: подробная демонстрация результатов работы, отчет о проделанной работе.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/5603
Защита программных реализаций от исследования.
Цели: получение навыков построения защиты программных реализаций от исследования.
Содержание: организация динамического изменения кода программы, искусственного усложнения структуры программы, нестандартного обращения к функциям операционной системы при реализации программы, искусственного усложнения алгоритмов обработки данных в программе, выявления факта выполнения программы под отладчиком.
Результаты: консольное приложение, реализующее решение поставленной задачи, подробная демонстрация результатов работы, отчет о проделанной работе.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/5603

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

Данный вид работы не предусмотрен УП.

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ

1. постановка задачи анализа программных реализаций

2. Какие этапы включает анализ программных реализаций?

3.

4. Каково описание, возможности, достоинства и недостатки метода экспериментов с "черным ящиком"?

5.

6. Как применять метод экспериментов с "черным ящиком" при анализе программных реализаций?

7.

8. Каково описание, возможности, достоинства и недостатки статического метода анализа программных реализаций?

9.

10. Как применять статический метод анализа программных реализаций на практике?

11.

12. Каково описание, возможности, достоинства и недостатки динамического метода анализа программных реализаций?

13.

14. Каковы основные методы поиска интересующей функции в программной реализации?

15.

16. Как применять метод маяков на практике?

17.

18. Как применять метод Step-Trace на практике?

19.

20. Каковы особенности анализа графических программ в ОС семейства Windows?

21.

22. Каковы возможности пакета утилит SysInternals?

23.

24. Как можно реализовать механизм обнаружения факта выполнения программы под отладчиком

25. какие стратегии могут быть применены для обхода механизмов защиты злоумышленниками при анализе защищенных программных реализаций

26. Введение промежуточного кода

27. Изменение последовательности выполнения

28. Использование ассемблерных вставок

29. Добавление бесполезного кода:

30. Использование сложных конструкций

31. Введение ложных путей выполнения

32. Использование трюков с указателями и манипуляциями с адресами памяти для обхода стандартных механизмов вызова функций.

33.

34. Использование syscalls вместо стандартных библиотечных функций.

35.

36. В чем заключаются основные вызовы и ограничения при попытке анализа и декомпиляции программного кода, который подвергся искусственному усложнению алгоритмов обработки данных?

37.

38. методы искусственного усложнения алгоритмов обработки данных

39. Каковы представления о работе с отладчиками уровня ядра?

40.

41. Каковы особенности анализа оверлейных программ?

42.

43. Каковы достоинства, недостатки и принципы функционирования каждой формальной модели взаимодействия программной закладки и атакуемой системы ("наблюдатель", "перехват", "искажение")?

44.

45. Каковы основные формальные модели взаимодействия программной закладки с атакуемой системой?

46.

47. Формальная модель "наблюдатель" в контексте взаимодействия программной закладки с атакуемой системой

48. Пример формальной модели "наблюдатель"

49. потенциальные риски и уязвимости могут возникнуть при использовании формальной модели "перехват"

50. меры противодействия формальной модели "перехват"

51. Как формальная модель "искажение" может быть реализована на уровне ядра операционной системы

52. Нетрадиционными методы защиты и анализа модели "искажение"

53. Каковы достоинства, недостатки и принципы функционирования каждого метода внедрения программных закладок (маскировка под прикладное и системное ПО, подмена системного ПО, метод прямого и косвенного ассоциирования с программным модулем)?

54.

55. Каковы основные методы внедрения программных закладок?

56.

57. классификация и особенности функционирования каждого класса программных закладок и вирусов?

58.

59. определение вируса и предъявляемые к нему требования?

60.

61. Каковы основные средства и методы защиты от программных закладок?

62.

63. Созданиеизолированногокомпьютера, как средство борьбы с закладками

64. Как организовать защиту от программных закладок и антивирусную защиту в компьютерной системе?

65.

66. Каковы основные организационные и административные меры антивирусной защиты?

67.

10. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩИХСЯ

Содержание, требования, условия и порядок организации самостоятельной работы обучающихся с учетом формы обучения определяются в соответствии с «Положением об организации самостоятельной работы обучающихся», утвержденным Ученым советом УлГУ (протокол №8/268 от 26.03.2019г.).

По каждой форме обучения: очная/заочная/очно-заочная заполняется отдельная таблица

Форма обучения: очная

Название разделов и тем	**Вид самостоятельной работы** ***(проработка учебного материала, решение задач, реферат, доклад, контрольная работа,подготовка к сдаче зачета, экзамена и др).***	**Объем в часах**	**Форма контроля** ***(проверка решения задач, реферата и др.)***
Раздел 1. Анализ программных реализаций			
Тема 1.1. Постановка задачи анализа программных реализаций.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование
Тема 1.2. Метод экспериментов с “черным ящиком”.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование
Тема 1.3. Статический метод.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование
Тема 1.4. Динамический метод.	Проработка учебного материала с	2	Тестирование

Название разделов и тем	**Вид самостоятельной работы** ***(проработка учебного материала, решение задач, реферат, доклад, контрольная работа,подготовка к сдаче зачета, экзамена и др).***	**Объем в часах**	**Форма контроля** ***(проверка решения задач, реферата и др.)***
	использованием ресурсов учебно-методического и информационного обеспечения дисциплины.		
Тема 1.5. Особенности анализа некоторых видов программ	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование
Раздел 2. Защита программных реализаций			
Тема 2.1. Постановка задачи защиты программных реализаций от изучения	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование
Тема 2.2. Динамическое изменение кода программы.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование
Тема 2.3. Искусственное усложнение структуры программы	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование
Тема 2.4. Нестандартные обращения к функциям операционной системы.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование
Тема 2.5. Искусственное усложнение алгоритмов обработки данных	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование
Тема 2.6. Выявление факта выполнения программы под отладчиком.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование
Раздел 3. Программные закладки, пути их внедрения, средства и методы противодействия программным закладкам			
Тема 3.1. Программные закладки и формальные модели	Проработка учебного материала с использованием ресурсов учебно-	4	Тестирование

Название разделов и тем	**Вид самостоятельной работы** ***(проработка учебного материала, решение задач, реферат, доклад, контрольная работа,подготовка к сдаче зачета, экзамена и др).***	**Объем в часах**	**Форма контроля** ***(проверка решения задач, реферата и др.)***
их взаимодействия с атакуемой системой.	методического и информационного обеспечения дисциплины.		
Тема 3.2. Формальная модель “наблюдатель”.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование
Тема 3.3. Формальная модель “перехват”.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование
Тема 3.4. Формальная модель “искажение”.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование
Тема 3.5. Методы внедрения программных закладок.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование
Тема 3.6. Компьютерные вирусы	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование
Тема 3.7. Средства и методы защиты от программных закладок	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование
Тема 3.8. Организационные и административные меры антивирусной защиты.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование

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 / О. В. Казарин, А. С. Забабурин. - Москва : Юрайт, 2024. - 312 с. - (Высшее образование). - URL: https://urait.ru/bcode/538066 . - Режим доступа: Электронно-библиотечная система Юрайт, для авториз. пользователей. - ISBN 978-5-9916-9043-0 : 1289.00. / .— ISBN 0_524832

2. Этапы формирования модели угроз и модели нарушителя информационной безопасности с учетом изменений законодательства Российской Федерации : учебное пособие / О. М. Голембиовская, М. Ю. Рытов, К. Е. Шинаков [и др.] ; О. М. Голембиовская, М. Ю. Рытов, К. Е. Шинаков [и др.]. - Саратов : Вузовское образование, 2021. - 265 с. - Книга находится в премиум-версии ЭБС IPR BOOKS. - Текст. - Весь срок охраны авторского права. - электронный. - Электрон. дан. (1 файл). - URL: http://www.iprbookshop.ru/109162.html. - Режим доступа: ЭБС IPR BOOKS; для авторизир. пользователей. - ISBN 978-5-4487-0791-9. / .— ISBN 0_269333

дополнительная

1. Борисов А.Б. КОММЕНТАРИЙ К ГРАЖДАНСКОМУ КОДЕКСУ РОССИЙСКОЙ ФЕДЕРАЦИИ ЧАСТИ ЧЕТВЕРТОЙ (ПОСТАТЕЙНЫЙ). ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОТНОШЕНИЙ В СФЕРЕ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ. С ПОСТАТЕЙНЫМИ МАТЕРИАЛАМИ И ПРАКТИЧЕСКИМИ РАЗЪЯСНЕНИЯМИ : практическое пособие / А.Б. Борисов ; Борисов А.Б. - Москва : Книжный мир, 2007. - 288 с. - URL: https://www.studentlibrary.ru/book/ISBN9785804102860.html. - Режим доступа: ЭБС "Консультант студента"; по подписке. - ISBN 978-5-8041-0286-0. / .— ISBN 0_236484

2. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин ; В. Ф. Шаньгин. - Саратов : Профобразование, 2019. - 702 с. - Книга находится в премиум-версии ЭБС IPR BOOKS. - Текст. - Лицензия до 24.09.2024. - электронный. - Электрон. дан. (1 файл). - URL: http://www.iprbookshop.ru/87995.html. - Режим доступа: ЭБС IPR BOOKS; для авторизир. пользователей. - ISBN 978-5-4488-0070-2. / .— ISBN 0_149907

учебно-методическая

1. Сутыркина Е. А. Методические указания к лабораторным работам по дисциплине «Анализ уязвимостей программного обеспечения» 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. - 2020. - Загл. с экрана. - Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 1,1 МБ). - Режим доступа: ЭБС УлГУ. - Текст : электронный. / .— ISBN 0_37913.

2. Сутыркина Е. А. Анализ уязвимостей программного обеспечения : методические указания для самостоятельной работы студентов по специальности 10.05.03 «Информационная безопасность автоматизированных систем» / Е. А. Сутыркина ; УлГУ, ФМИиАТ. - 2024. - Неопубликованный ресурс. - URL: https://lib.ulsu.ru/MegaPro/Download/MObject/16664. - Режим доступа: ЭБС УлГУ. - Текст : электронный. / .— ISBN 0_599881.

б) Программное обеспечение

- Операционная система "Альт образование"
- Офисный пакет "Мой офис"
- Альт рабочая станция
- Академическая лицензия на УМК ViPNet "Защита сетей"
- Комплект «Максимальная защита» Средства защиты информации Secret Net Studio 8

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, [2024]. – 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, [2024]. - 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, [2024]. – 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, [2024]. – URL: https://www.rosmedlib.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО Букап. – Томск, [2024]. – 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, [2024]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. ЭБС **Znanium.com** : электронно-библиотечная система : сайт / ООО Знаниум. - Москва, [2024]. - 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, [2024].

3. eLIBRARY.RU: научная электронная библиотека : сайт / ООО «Научная Электронная Библиотека». – Москва, [2024]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

4. Федеральная государственная информационная система «Национальная электронная библиотека» : электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2024]. – 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.

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

Аудитории для проведения лекций, семинарских занятий, для выполнения лабораторных работ и практикумов, для проведения текущего контроля и промежуточной аттестации, курсового проектирования, групповых и индивидуальных консультаций *(выбрать необходимое)*

Аудитории укомплектованы специализированной мебелью, учебной доской. Аудитории для проведения лекций оборудованы мультимедийным оборудованием для представления информации большой аудитории. Помещения для самостоятельной работы оснащены компьютерный техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде, электронно-библиотечной системе. Перечень оборудования, используемого в учебном процессе:

- Мультимедийное оборудование: компьютер/ноутбук, экран, проектор/телевизор
- Компьютерная техника

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 одни 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 Кандидат физико-математических наук	Сутыркина Екатерина Алексеевна
	Должность, ученая степень, звание	ФИО