**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 | Анализ уязвимостей программного обеспечения |
| Факультет | Математики, информационных и авиационных технологий |
| Кафедра | Информационной безопасности и теории управления |
| Курс | 4 |

Специальность: 10.05.03 «Информационная безопасность автоматизированных систем»
*код направления (специальности), полное наименование*

Специализация: «Безопасность открытых информационных систем»
*полное наименование*

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

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

Программа актуализирована на заседании кафедры: протокол № 12 от 12.04.2023 г.
Программа актуализирована на заседании кафедры: протокол № 10 от 15.04.2024 г.
Программа актуализирована на заседании кафедры: протокол № __ от _____ 20____г.

| 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. /<br>*(подпись)* *(Ф.И.О.)*<br>« 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;

**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 относится к числу вариативных дисциплин в рамках образовательной программы и читается в 8-м семестре студентам специальности «Информационная безопасность автоматизированных систем» очной формы обучения.

Для успешного изучения дисциплины необходимы знания и умения, приобретенные в результате освоения курсов «Вычислительные методы в алгебре и теории чисел», «Теоретико-числовые методы в криптографии», «Математические модели информационных систем», «Компьютерные сети», «Инструментальные средства контроля защищенности информации», «Технические средства обнаружения каналов утечки информации».

Результаты освоения дисциплины будут необходимы для дальнейшего процесса обучения в рамках поэтапного формирования компетенций при изучении следующих дисциплин: «Теория кодирования, сжатия и восстановления информации», «Методы алгебраической геометрии в криптографии», «Аттестация объектов информатизации», а также для прохождения практик 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** |
|---|---|
| ПК-3 Способен разрабатывать проектные решения по защите информации в автоматизированных системах | **Знает:**<br>Критерии оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем<br>**Умеет:**<br>Определять методы управления доступом, типы доступа и |

| | |
|---|---|
| | правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе<br>**Владеет:**<br>Навыками разработки предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах |
| ПК-6 Способен проводить контроль защищенности информации от НСД | **Знает:**<br>Методы защиты информации и методики контроля защищенности информации от несанкционированного доступа и специальных программных воздействий на нее<br>**Умеет:**<br>Проводить оценку защищенности информации от несанкционированного доступа и специальных воздействий<br>Проверять работоспособность средств защиты информации от несанкционированного доступа и специальных воз-действий, выполнение правил их эксплуатации<br>**Владеет:**<br>Навыками проведения контроля защищенности информации от несанкционированного доступа и специальных воздействий |

## 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 | 36/36* | | |
| •Практические и семинарские занятия | | | | |
| •Лабораторные работы (лабораторный практикум) | 18 | 18/18* | | |
| Самостоятельная работа | 54 | 54 | | |
| Форма текущего контроля знаний и контроля самостоятельной работы | | Лабораторные работы, тестирование | | |
| Курсовая работа | | | | |
| Всего часов по дисциплине | 108 | 108 | | |

| | | | | |
|---|---|---|---|---|
| Виды промежуточной аттестации (экзамен, зачет) | Зачёт | зачет | | |
| Общая трудоемкость в зач. ед. | 3 | 3 | | |

**В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий в таблице через слеш указывается количество часов работы ППС с обучающимися для проведения занятий в дистанционном формате с применением электронного обучения*

**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. Анализ программных реализаций** | | | | | | | |
| 1. Постановка задачи анализа программных реализаций. | | 1 | | 0 | | 4 | тестирование |
| 2. Метод экспериментов с “черным ящиком”. | | 2 | | 1* | * | 2 | лабораторная работа, тестирование |
| 3.Статический метод. | | 2 | | 1* | * | 2 | лабораторная работа, тестирование |
| 4.Динамический метод. | | 2 | | 1* | * | 2 | лабораторная работа, тестирование |
| 5.Особенности анализа некоторых видов программ | | 2 | | 1 | | 4 | лабораторная работа, тестирование |
| **Раздел 2. Защита программных реализаций** | | | | | | | |
| 6. Постановка задачи защиты программных реализаций от изучения. | | 1 | | 0 | | 4 | тестирование |
| 7. Динамическое изменение кода программы. | | 2 | | 1* | * | 2 | лабораторная работа, тестирование |
| 8.Искусственное усложнение структуры программы | | 2 | | 1* | * | 2 | лабораторная работа, тестирование |
| 9.Нестандартные обращения к функциям операционной системы. | | 2 | | 1* | * | 2 | лабораторная работа, тестирование |
| 10.Искусственное | | 2 | | 1* | * | 2 | лабораторная |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| усложнение алгоритмов обработки данных | | | | | | | работа, тестирование |
| 11.Выявление факта выполнения программы под отладчиком. | | 2 | | 1* | * | 2 | лабораторная работа, тестирование |
| **Раздел 3. Программные закладки, пути их внедрения, средства и методы противодействия программным закладкам** | | | | | | | |
| 12. Программные закладки и формальные модели их взаимодействия с атакуемой системой. | | 2 | | 0 | | 4 | тестирование |
| 13. Формальная модель “наблюдатель”. | | 2 | | 1* | * | 2 | лабораторная работа, тестирование |
| 14. Формальная модель “перехват”. | | 2 | | 1* | * | 2 | лабораторная работа, тестирование |
| 15. Формальная модель “искажение”. | | 2 | | 1* | * | 2 | лабораторная работа, тестирование |
| 16. Методы внедрения программных закладок. | | 2 | | 1 | | 4 | лабораторная работа, тестирование |
| 17. Компьютерные вирусы. | | 2 | | 2 | | 4 | лабораторная работа, тестирование |
| 18. Средства и методы защиты от программных закладок. | | 2 | | 1 | | 4 | лабораторная работа, тестирование |
| 19. Организационные и административные меры антивирусной защиты. | | 2 | | 2* | * | 4 | лабораторная работа, тестирование |
| Зачет | | | | | | | |
| | | | | | | | |
| Итого | 108 | 36 | | 18 | (18*) | 54 | |

*-занятия проводятся в интерактивной форме

## 5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

### Раздел 1. Анализ программных реализаций.

**Тема 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 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 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 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 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.

**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 6. 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 7. 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 8.** 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 9.** 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 10.** Выявление факта выполнения программы под отладчиком. Способы выявления факта выполнения программы под отладчиком. Использование функции IsDebuggerPresent. Проверка контрольных сумм участков кода, которые не должны изменяться в ходе обычного выполнения программы. Отслеживание длительности выполнения тех или иных участков кода программы. Навязывание отладчику ложных точек останова. Засорение консоли отладчика многократными вызовами системной функции OutputDebugString.

**Тема 11.** Выявление конкретных отладчиков по косвенным признакам. 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 12. 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 13. 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 14. 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 15. 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 16. 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 17. 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 18. Средства и методы защиты от программных закладо**к. 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 19. 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

Практические и семинарские занятия не предусмотрены учебным планом.

## 7. ЛАБОРАТОРНЫЕ РАБОТЫ (ЛАБОРАТОРНЫЙ ПРАКТИКУМ)

Цикл лабораторных работ включает в себя 3 объемных лабораторных работы. Задачами цикла являются:

- освоение основных методов анализа программных реализаций на практике;
- освоение принципов работы с современными дизассемблерами и отладчиками;
- освоение основных методов защиты программных реализаций от анализа;
- освоение основных методов организации защиты от программных закладок и вирусов в компьютерных системах.

Лабораторная 1. **Повторение. Основы работы с ассемблером.**

Цель: повторение основных элементов языка ассемблера и соответствующих приемов работы с ассемблером.

Содержание работы: 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.

Результат: консольное приложение, реализующее решение поставленной задачи.

Методические указания: выполнение задания должно вестись с использованием ассемблеров и IDE сред разработки.

Лабораторная 2. **Анализ программных реализаций.** Цель: получение навыков анализа программных реализаций, работы с отладчиками и дизассемблерами.

Содержание работы: 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.

Результат: подробная демонстрация результатов работы, отчет о проделанной работе.

Методические указания: выполнение задания должно вестись с использованием дизассемблеров, отладчиков, и вспомогательных программных средств,, отчет должен содержать подробный анализ проделанной работы.

Лабораторная 3. **Защита программных реализаций от исследования.**

Цель: получение навыков построения защиты программных реализаций от исследования.

Содержание работы: 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.

Результат: консольное приложение, реализующее решение поставленной задачи, подробная демонстрация результатов работы, отчет о проделанной работе.

Методические указания: выполнение задания должно вестись с использованием ассемблеров, дизассемблеров, отладчиков и IDE сред разработки, отчет должен содержать подробный анализ проделанной работы.

## 8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

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

## 9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ

1. Знать постановку задачи анализа программных реализаций.
2. Знать этапы анализа программных реализаций.
3. Знать описание, возможности, достоинства и недостатки метода экспериментов с “черным ящиком”.
4. Уметь применять метод экспериментов с “черным ящиком” при анализе программных реализаций.
5. Знать описание, возможности, достоинства и недостатки статического метода анализа программных реализаций.
6. Уметь применять статический метод анализа программных реализаций на практике.
7. Уметь работать с дизассемблерами.

8. Знать описание, возможности, достоинства и недостатки динамического метода анализа программных реализаций.
9. Знать основные методы поиска интересующей функции в программной реализации.
10. Уметь применять метод маяков на практике.
11. Уметь применять метод Step-Trace на практике.
12. Уметь применять динамический метод анализа программных реализаций на практике.
13. Иметь представление о механизмах работы отладчика.
14. Уметь работать с отладчиками программных реализаций.
15. Иметь представления о работе с отладчиками уровня ядра.
16. Знать особенности анализа оверлейных программ.
17. Знать особенности анализа графических программ в ОС семейства Windows.
18. Иметь представления о возможностях пакета утилит SysInternals.
19. Знать постановку задачи защиты программных реализаций от изучения.
20. Знать достоинства и недостатки защиты программных реализаций от анализа.
21. Знать основные способы защиты программных реализаций от анализа (динамическое изменение кода программы, искусственное усложнение структуры программы, нестандартное обращение к функциям операционной системы, искусственное усложнения алгоритмов обработки данных, выявление факта выполнения программы под отладчиком).
22. Уметь реализовать защиту программной реализации от анализа на практике.
23. Иметь представления о субъектно-ориентированной модели компьютерной системы.
24. Знать определение программной закладки и предъявляемые к ней требования.
25. Знать основные формальные модели взаимодействия программной закладки с атакуемой системой.
26. Знать достоинства, недостатки и принципы функционирования каждой формальной модели взаимодействия программной закладки и атакуемой системы (“наблюдатель”, ”перехват”, ”искажение”).
27. Знать основные методы внедрения программных закладок.
28. Знать 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).
29. Знать определение вируса и предъявляемые к нему требования.
30. Знать классификацию и особенности функционирования каждого класса программных закладок и вирусов.
31. Знать основные средства и методы защиты от программных закладок.
32. Знать основные организационные и административные меры антивирусной защиты.
33. Уметь организовать защиту от программных закладок и антивирусную защиту в компьютерной системе.

## 10. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

| **Название разделов и тем** | **Вид самостоятельной работы** | **Объем в часах** | **Форма контроля** |
|---|---|---|---|
| 1. Постановка задачи анализа программных реализаций. | Проработка учебного материала, подготовка к сдаче зачета | 4 | Зачет, тестирование |
| 2. Метод экспериментов с “черным ящиком”. | Проработка учебного материала, подготовка к сдаче зачета, лабораторные | 2 | Лабораторная работа, зачет, тестирование |

| | | | |
| --- | --- | --- | --- |
| | работы | | |
| 3. Статический метод. | Проработка учебного материала, подготовка к сдаче зачета, лабораторные работы | 2 | Лабораторная работа, зачет, тестирование |
| 4. Динамический метод. | Проработка учебного материала, подготовка к сдаче зачета, лабораторные работы | 2 | Лабораторная работа, зачет, тестирование |
| 5. Особенности анализа некоторых видов программ. | Проработка учебного материала, подготовка к сдаче зачета, лабораторные работы | 4 | Лабораторная работа, зачет, тестирование |
| 6. Постановка задачи защиты программных реализаций от изучения. | Проработка учебного материала, подготовка к сдаче зачета | 4 | Зачет , тестирование |
| 7. Динамическое изменение кода программы. | Проработка учебного материала, подготовка к сдаче зачета, лабораторные работы | 2 | Лабораторная работа, зачет, тестирование |
| 8. Искусственное усложнение структуры программы. | Проработка учебного материала, подготовка к сдаче зачета, лабораторные работы | 2 | Лабораторная работа, зачет, тестирование |
| 9. Нестандартные обращения к функциям операционной системы. | Проработка учебного материала, подготовка к сдаче зачета, лабораторные работы | 2 | Лабораторная работа, зачет, тестирование |
| 10. Искусственное усложнение алгоритмов обработки данных. | Проработка учебного материала, подготовка к сдаче зачета, лабораторные работы | 2 | Лабораторная работа, зачет, тестирование |
| 11. Выявление факта выполнения программы под отладчиком. | Проработка учебного материала, подготовка к сдаче зачета, лабораторные работы | 2 | Лабораторная работа, зачет, тестирование |
| 12. Программные закладки и формальные модели их взаимодействия с атакуемой системой. | Проработка учебного материала, подготовка к сдаче зачета | 4 | Зачет , тестирование |
| 13. Формальная модель “наблюдатель”. | Проработка учебного материала, подготовка к сдаче зачета, лабораторные работы | 2 | Лабораторная работа, зачет, тестирование |
| 14. Формальная модель “перехват”. | Проработка учебного материала, подготовка к сдаче зачета, лабораторные работы | 2 | Лабораторная работа, зачет, тестирование |
| 15. Формальная модель | Проработка учебного | 2 | Лабораторная |

| | | | |
|---|---|---|---|
| “искажение”. | материала, подготовка к сдаче зачета, лабораторные работы | | работа, зачет, тестирование |
| 16. Методы внедрения программных закладок. | Проработка учебного материала, подготовка к сдаче зачета, лабораторные работы | 4 | Лабораторная работа, зачет, тестирование |
| 17. Компьютерные вирусы. | Проработка учебного материала, подготовка к сдаче зачета, лабораторные работы | 4 | Лабораторная работа, зачет, тестирование |
| 18. Средства и методы защиты от программных закладок. | Проработка учебного материала, подготовка к сдаче зачета, лабораторные работы | 4 | Лабораторная работа, зачет, тестирование |
| 19. Организационные и административные меры антивирусной защиты. | Проработка учебного материала, подготовка к сдаче зачета, лабораторные работы | 4 | Лабораторная работа, зачет, тестирование |

## 11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

**а) Список рекомендуемой литературы**

**основная**

1. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/531084
2. Федин, Ф. О. Информационная безопасность баз данных : учебное пособие / Ф. О. Федин, О. В. Трубиенко, С. В. Чискидов. — Москва : РТУ МИРЭА, 2020 — Часть 1 — 2020. — 133 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167605

**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. Автор комментариев и составитель - А.Б. Борисов - м.: книжный мир, 2007. - 288 с. - isbn 978-5-8041-0286-0 — URL: http://www.studentlibrary.ru/book/isbn9785804102860.html
2.Щербаков А.Ю., А.Ю. Щербаков. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Учебное пособие. - М.: Книжный мир, 2009. - 352 с. - ISBN 978-5-8041-0378-2]. — URL: http://www.studentlibrary.ru/book/ISBN9785804103782.html
3.Аверченков, В. И. Защита персональных данных в организации : монография / В. И. Аверченков, М. Ю. Рытов, Т. Р. Гайнулин. — Брянск : Брянский государственный технический университет, 2012. — 124 с. — ISBN 5-89838-382-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/6993.html

**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, ФМИиАТ. - Ульяновск : УлГУ, 2019. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 1,10 МБ). — URL: http://lib.ulsu.ru/MegaPro/Download/MObject/5603

Согласовано:

Ведущий специалист НБ УлГУ / Терехина Л.А. / _____ / 04.05.2023 /
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 :

- RadASM,
- WinAsm Studio,
- MS MASM,
- fasm,
- NASM,
- Hex-Rays IDA Pro Disassembler,
- OllyDbg.
- MS WinDbg,
- SysInternals,
- Qt Creator / Qt,
- Eclipse CDT.

**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:

- RadASM,
- WinAsm Studio,
- MS MASM,
- fasm,
- NASM,
- Hex-Rays IDA Pro Disassembler,
- OllyDbg.
- MS WinDbg,
- SysInternals,
- Qt Creator / Qt,
- Eclipse CDT.

## 13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

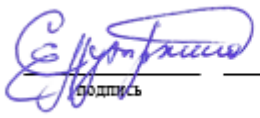
В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться некоторые из следующих вариантов восприятия информации с учетом их индивидуальных психофизических особенностей:

– 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

**ЛИСТ ИЗМЕНЕНИЙ**

| № п/п | Содержание изменения или ссылка на прилагаемый текст изменения | ФИО заведующего кафедрой, реализующей дисциплину/выпускающей кафедрой | Подпись | Дата |
|---|---|---|---|---|
| 1. | Утверждение РПД и ФОС для набора 2023 года (10.05.01 и 10.05.03). Актуализация РПД и ФОС для наборов 2022 года 10.05.01 и 10.05.03 (без изменений) | Андреев А.С. |  | 12.04.2023 Протокол заседания кафедры № 12 |
| 2. | Утверждение РПД и ФОС для набора 2024 года (10.05.03). Актуализация РПД и ФОС для наборов 2023 года 10.05.01 и 10.05.03 (без изменений) | Андреев А.С. |  | 15.04.2024 Протокол заседания кафедры № 10 |