УП2013

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)

УТВЕРЖДАЮ
Проректор
по образовательной деятельности
_____ А.А.Панфилов
«29» 12 _____ 2016 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ
(наименование дисциплины)

Специальность 10.05.04 "Информационно-аналитические системы безопасности"

Специализация "Автоматизация информационно-аналитической деятельности"

Уровень высшего образования специалитет

Форма обучения очная

Семестр	Трудоемкость зач. ед,/ час.	Лекции, час.	Практич. занятия, час.	Лаборат. работы, час.	СРС, час.	Форма промежуточного контроля (экз./зачет)
4	4/144	36		36	36	Экзамен (36ч), КР
Итого	4/144	36		36	36	Экзамен (36ч), КР

Владимир 2016

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины «Безопасность операционных систем» являются обеспечение подготовки специалистов в соответствии с требованиями ФГОС ВО и учебного плана по направлению 10.05.04 «Информационно-аналитические системы безопасности», ознакомление студентов с основными методами и технологиями, назначением и функционированием механизмов обеспечения информационной безопасности операционных систем (ОС), углубленное изучение внутреннего устройства и алгоритмов работы основных компонентов современных операционных систем MS Windows, и UNIX, освоение функций системного программного интерфейса Win32 API и принципов обеспечения безопасности для ОС MS Windows.

Задачами освоения дисциплины «Безопасность операционных систем» является изучение следующих вопросов и тем:

-организации процессов и потоков, моделирование режима многозадачности. Потоки в POSIX. Реализация потоков в пользовательском пространстве, в ядре, гибридная реализация;

- взаимодействия процессов. Критические области. Синхронизационные примитивы;

- планирование в пакетных системах и в интерактивных системах. Системы реального времени. Планирование потоков. Классические задачи взаимодействия процессов;

-вопросы управление памятью. Страничная организация памяти, таблицы страниц. Алгоритмы замещения страниц: алгоритм LRU, алгоритм WSClock, алгоритм "рабочий набор";

изучение системы страничной организации памяти. Сегментация со страничной организацией памяти;

- файловые системы. Файловые системы с журнальной структурой. Журналируемые файловые системы. Оценка производительности ФС;

- ПО ввода-вывода. Ввод-вывод, управляемый прерываниями. Ввод-вывод с помощью DMA. Обработчики прерываний, драйверы устройств. Слой абстракции от оборудования (HAL);

- взаимоблокировка. Выгружаемые и невыгружаемые ресурсы. Условия возникновения ресурсных взаимоблокировок. Обнаружение взаимоблокировок разных типов. Уклонение от взаимоблокировок;

-технологии виртуализации. Гипервизоры первого и второго типа. Аппаратная поддержка вложенных таблиц страниц. Домены устройств;

-виртуальные машины на мультиядерных центральных процессорах. Виртуализация на примере продуктов VmWare;

-управление доступом к ресурсам. Реализация формальных моделей безопасности в операционных системах. Криптопроцессоры и криптопровайдеры. Аутентификация и авторизация в современных операционных системах;

- атаки переполнения буфера. Атаки, использующие форматирующую строку. Указатели на несуществующие объекты. Атаки, использующие внедрение команд. Инсайдерские атаки. Вредоносные программы;

-брандмауэры. Антивирусные технологии. Электронная подпись программ. Инкапсулированный код. Современные исследования в области безопасности операционных систем и т.д.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО СПЕЦИАЛИТЕТА

Данная дисциплина относится к базовой части Блока Б1 (Б1.Б.4). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций и практических занятий.

Дисциплина изучается на 2 курсе, требования к «входным» знаниям, умениям и готовностям (пререквизитам) обучающегося определяются требованиями к уровню подготовки по специальности 10.05.04 «Информационно-аналитические системы безопасности», квалификации - специалист по курсам «Информатика», «Основы информационной безопасности», «Аппаратные средства вычислительной техники», «Структуры данных», «Технологии и методы программирования», «Введение в специальность». Курс тесно взаимосвязан с другими дисциплинами. Он является базовым для изучения таких дисциплин

как «Безопасность информационных и аналитических систем», «Безопасность электронного документооборота», «Базы данных и экспертные системы», «Программно-аппаратные средства защиты информации», «Администрирование сетей» и т.д.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате освоения дисциплины студент должен обладать следующими общепрофессиональными компетенциями:

ОПК-3 – способностью применять в профессиональной деятельности современные средства вычислительной техники и программное обеспечение, достижения информационных технологий для поиска и обработки информации по профилю профессиональной деятельности;

профессиональными компетенциями:

ПК-10 – способностью осуществлять выбор технологии, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности создаваемых специальных ИАС.

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

1) **Знать:** - аппаратные средства вычислительной техники; -эталонную модель взаимодействия открытых систем, методы коммутации и маршрутизации, сетевые протоколы; - основные виды политик управления доступом и информационными потоками в компьютерных системах;- защитные механизмы и средства обеспечения безопасности операционных систем; - средства и методы хранения и передачи аутентификационной информации; - требования к подсистеме аудита и политике аудита; - основы системного программирования; - принципы построения современных операционных систем и особенности их применения; - основные виды и угрозы безопасности операционных систем (ОПК-3; ПК-10);

2) **Уметь:** -выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах; - формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе; - осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; - применять основные виды политик управления доступом и информационными потоками в компьютерных системах; - основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков; - работать с интегрированной средой разработки программного обеспечения; - разрабатывать частные политики безопасности компьютерных систем, в том числе, политики управления доступом и информационными потоками (ОПК-3; ПК-10);

3) **Владеть:** - разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками; - навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств; - навыками системного программирования; - навыками конфигурирования и администрирования операционных систем - профессиональной терминологией в области информационной безопасности (ОПК-3; ПК-10).

У обучаемых в процессе изучения дисциплины должны вырабатываться дополнительные компетенции, с учетом требований работодателей:

- способность применять навыки использования специальных программных средств для защиты операционных систем от вредоносных программ и атак.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 4 зачетных единиц, 144 часа.

№ п/п	Раздел (тема) дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)						Объем учебной работы, с применением интерактивных методов (в часах / %)	Формы текущего контроля успеваемости *(по неделям семестра)*, форма промежуточной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	Контрольные работы	СРС	КП / КР		
1.	Введение. Понятия операционной системы: процесс, адресное пространство, файл, ввод-вывод, шины. Системные вызовы.	4	1	2		2		2		2/50%	
2.	Процессы и потоки. Модель процесса, состояние процессов, моделирование режима многозадачности.	4	2	2		2		2		1/25%	
3.	Взаимодействие процессов. Состязательные ситуации. Критические области. Синхронизационные примитивы	4	3	2		2		2		2/50%	
4.	Планирование в пакетных системах. Планирование в интерактивных системах. Системы реального времени.	4	4	2		2		2		1/25%	
5.	Управление памятью. Виртуальная память. Страничная организация памяти, таблицы страниц.	4	5	2		2		2		1/25%	
6.	Системы страничной организации памяти. Управление загрузкой. Разделение пространства команд и данных.	4	6	2		2		2		2/50%	Рейтинг-контроль №1
7.	Файловые системы. Свойства файлов. Файловые системы с журнальной структурой.	4	7	2		2		2		1/25%	
8.	Ввод и вывод информации. Устройства и контроллеры устройств ввода-вывода.	4	8	2		2		2		1/25%	

№ п/п	Раздел (тема) дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)						Объем учебной работы, с применением интерактивных методов (в часах / %)	Формы текущего контроля успеваемости *(по неделям семестра)*, форма промежу-точной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	Контрольные работы	СРС	КП / КР		
9.	ПО ввода-вывода. Ввод-вывод, управляемый прерываниями. Ввод-вывод с помощью DMA. Обработчики прерываний, драйверы устройств.	4	9	2		2		2		1/25%	
10.	Аппаратная часть дисков. Алгоритмы планирования перемещения блока головок. Обработка ошибок.	4	10	2		2		2		2/50%	
11.	Взаимоблокировка. Выгружаемые и невыгружаемые ресурсы. Условия возникновения ресурсных взаимоблокировок.	4	11	2		2		2		1/25%	
12.	Предотвращение взаимоблокировки. Атака условия взаимного исключения. Атака условия удержания и ожидания.	4	12	2		2		2		1/25%	Рейтинг-контроль №2
13.	Технологии виртуализации. Гипервизоры первого и второго типа. Аппаратная поддержка вложенных таблиц страниц. Возвращение памяти.	4	13	2		2		2		1/25%	
14.	Виртуальные машины на мультиядерных центральных процессорах. Облака в качестве услуги.	4	14	2		2		2		2/50%	
15.	Многопроцессорные системы. Низкоуровневые коммуникационные программы мультикомпьютеров	4	15	2		2		2		2/50%	
16.	Управление доступом к ресурсам. Реализация формальных моделей безопасности в	4	16	2		2		2		2/50%	

№ п/п	Раздел (тема) дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)						Объем учебной работы, с применением интерактивных методов (в часах / %)	Формы текущего контроля успеваемости *(по неделям семестра)*, форма промежу-точной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	Контрольные работы	СРС	КП / КР		
	операционных системах. Реализация криптографических схем в ОС.										
17.	Атаки переполнения буфера. Атаки, использующие форматирующую строку. Указатели на несуществующие объекты. Разыменование нулевого указателя.	4	17	2		2		2		2/50%	
18.	Брандмауэры. Антивирусные технологии. Электронная подпись программ.	4	18	2		2		2		2/50%	Рейтинг-контроль №3
Всего				36		36		36	КР	27/38%	Экзамен

Содержание дисциплины «Безопасность операционных систем»

Раздел 1. Введение. Понятия операционной системы: процесс, адресное пространство, файл, ввод-вывод, шины. Системные вызовы. Монолитные системы, микроядра, виртуальные машины.

Раздел 2. Процессы и потоки. Модель процесса, состояние процессов, моделирование режима многозадачности. Потоки в POSIX. Реализация потоков в пользовательском пространстве, в ядре, гибридная реализация. Алгоритм активации планировщика.

Раздел 3. Взаимодействие процессов. Состязательные ситуации. Критические области. Синхронизационные примитивы: семафор, мьютекс, монитор. Барьеры. Передача сообщений.

Раздел 4. Планирование в пакетных системах. Планирование в интерактивных системах. Системы реального времени. Планирование потоков. Классические задачи взаимодействия процессов.

Раздел 5. Управление памятью. Виртуальная память. Страничная организация памяти, таблицы страниц. Алгоритмы замещения страниц: алгоритм LRU, алгоритм WSClock, алгоритм "рабочий набор".

Раздел 6. Системы страничной организации памяти. Управление загрузкой. Разделение пространства команд и данных. Совместно используемые страницы и библиотеки. Политика очистки страниц. Интерфейс виртуальной памяти. Сегментация со страничной организацией памяти.

Раздел 7. Файловые системы. Свойства файлов. Файловые системы с журнальной структурой. Журналируемые файловые системы. Виртуальные файловые системы. Непротиворечивость ФС. Оценка производительности ФС.

Раздел 8. Ввод и вывод информации. Устройства и контроллеры устройств ввода-вывода. Ввод-вывод, отображаемый на адресное пространство. Прямой доступ к памяти.

Раздел 9. ПО ввода-вывода. Ввод-вывод, управляемый прерываниями. Ввод-вывод с помощью DMA. Обработчики прерываний, драйверы устройств. Слой абстракции от оборудования (HAL).

Раздел 10. Аппаратная часть дисков. Алгоритмы планирования перемещения блока головок. Обработка ошибок. Аппаратная составляющая часов. Программируемые таймеры. Пользовательский интерфейс ввода-вывода. Управление энергопотреблением.

Раздел 11. Взаимоблокировка. Выгружаемые и невыгружаемые ресурсы. Условия возникновения ресурсных взаимоблокировок. Обнаружение взаимоблокировок разных типов. Уклонение от взаимоблокировок, алгоритм банкира.

Раздел 12. Предотвращение взаимоблокировки. Атака условия взаимного исключения. Атака условия удержания и ожидания. Атака условия невыгружаемости. Атака условия циклического ожидания. Двухфазное блокирование. Активная взаимоблокировка. Зависание.

Раздел 13. Технологии виртуализации. Гипервизоры первого и второго типа. Аппаратная поддержка вложенных таблиц страниц. Возвращение памяти. Виртуализация ввода-вывода. Блоки управления памятью при вводе-выводе. Домены устройств.

Раздел 14. Виртуальные машины на мультиядерных центральных процессорах. Облака в качестве услуги. Миграция виртуальных машин. Установка контрольных точек. Виртуализация на примере продуктов VmWare.

Раздел 15. Многопроцессорные системы. Низкоуровневые коммуникационные программы мультикомпьютеров. Распределенная совместно используемая память. Планирование мультикомпьютеров. Вызовы удаленных процедур. Балансировка нагрузки.

Раздел 16. Управление доступом к ресурсам. Реализация формальных моделей безопасности в операционных системах. Реализация криптографических схем в ОС. Криптопроцессоры и криптопровайдеры. Аутентификация и авторизация в современных операционных системах.

Раздел 17. Атаки переполнения буфера. Атаки, использующие форматирующую строку. Указатели на несуществующие объекты. Разыменование нулевого указателя. Переполнение целочисленных значений. Атаки, использующие внедрение команд. Инсайдерские атаки. Вредоносные программы.

Раздел 18. Брандмауэры. Антивирусные технологии. Электронная подпись программ. "Тюремное заключение". Обнаружение проникновения на основе модели. Инкапсулированный код. Современные исследования в области безопасности операционных систем.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Изучение дисциплины предполагает не только запоминание и понимание, но и анализ, синтез, рефлексию, формирует универсальные умения и навыки, являющиеся основой становления специалиста по специальности 10.05.04 «Информационно-аналитические системы безопасности».

Для реализации компетентностного подхода предлагается интегрировать в учебный процесс интерактивные образовательные технологии, включая информационные и коммуникационные технологии (ИКТ), при осуществлении различных видов учебной работы:

- учебную дискуссию;
- электронные средства обучения (слайд-лекции, электронные тренажеры, компьютерные тесты);
- дистанционные (сетевые) технологии.

Как традиционные, так и лекции инновационного характера могут сопровождаться компьютерными слайдами или слайд-лекциями. Основное требование к слайд-лекции – применение динамических эффектов (анимированных объектов), функциональным назначением которых является наглядно-образное представление информации, сложной для понимания и осмысления студентами, а также интенсификация и диверсификация учебного процесса.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью ОПОП специальности 10.05.04 «Информационно-аналитические системы безопасности», особенностью контингента обучающихся и содержанием конкретных дисциплин, и в целом, в учебном процессе, они составляют не менее 30 процентов аудиторных занятий.

Занятия лекционного типа для соответствующих групп студентов согласно требованиям стандарта высшего образования не могут составлять более 55 процентов аудиторных занятий. Программа дисциплины соответствует данным требованиям.

Таким образом, применение интерактивных образовательных технологий придает инновационный характер практически всем видам учебных занятий, включая лекционные. При этом делается акцент на развитие самостоятельного, продуктивного мышления, основанного на диалогических дидактических приемах, субъектной позиции обучающегося в образовательном процессе. Тем самым создаются условия для реализации компетентностного подхода при изучении данной дисциплины.

6. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Для текущего контроля успеваемости предлагается использование рейтинговой системы оценки, которая носит интегрированный характер и учитывает успешность студента в различных видах учебной деятельности, степень сформированности у студента общекультурных и профессиональных компетенций.

Примерный перечень заданий для текущих контрольных мероприятий:

Вопросы рейтинг-контроля №1

1. Понятие процесса.
2. Понятие адресного пространства.
3. Понятие файла.
4. Понятие ввода-вывода.
5. Понятие шины.
6. Системные вызовы.
7. Монолитные системы.
8. Микроядра.
9. Виртуальные машины.
10. Модель процесса.
11. Планирование в интерактивных системах.

12. Планирование в системах реального времени.
13. Планирование потоков.
14. Классические задачи взаимодействия процессов.
15. Виртуальная память.
16. Страничная организация памяти.
17. Алгоритмы замещения страниц.
18. Алгоритм LRU.

Вопросы рейтинг-контроля №2

1. Алгоритм WSClock.
2. Алгоритм "рабочий набор".
3. Управление загрузкой.
4. Разделение пространства команд и данных.
5. Совместно используемые страницы и библиотеки.
6. Политика очистки страниц.
7. Интерфейс виртуальной памяти.
8. Сегментация со страничной организацией памяти.
9. Файловые системы. Свойства файлов.
10. Файловые системы с журнальной структурой.
11. Аппаратная составляющая часов. Программируемые таймеры.
12. Пользовательский интерфейс ввода-вывода - клавиатура, мышь, монитор.
13. Управление энергопотреблением.
14. Выгружаемые и невыгружаемые ресурсы.
15. Условия возникновения ресурсных взаимоблокировок.
16. Обнаружение взаимоблокировок разных типов.
17. Уклонение от взаимоблокировок, алгоритм банкира.
18. Атака условия взаимного исключения.
19. Атака условия удержания и ожидания.

Вопросы рейтинг-контроля №3

1. Атака условия невыгружаемости.
2. Атака условия циклического ожидания.
3. Двухфазное блокирование. Активная взаимоблокировка. Зависание.
4. Технологии виртуализации. Гипервизоры первого и второго типа.
5. Аппаратная поддержка вложенных таблиц страниц. Возвращение памяти.
6. Планирование мультикомпьютеров.
7. Вызовы удаленных процедур.
8. Балансировка нагрузки.
9. Реализация формальных моделей безопасности в операционных системах.
10. Реализация криптографических схем в ОС.
11. Криптопроцессоры и криптопровайдеры.
12. Аутентификация и авторизация в современных операционных системах.
13. Атаки переполнения буфера.
14. Атаки, использующие форматирующую строку.
15. Указатели на несуществующие объекты.
16. Разыменование нулевого указателя.
17. Переполнение целочисленных значений.
18. Атаки, использующие внедрение команд.
19. Антивирусные технологии.
20. Электронная подпись программ.
21. Защита кода типа "Тюремное заключение".
22. Обнаружение проникновения на основе модели.
103. Инкапсулированный код.

Перечень вопросов к экзамену (промежуточной аттестации по итогам освоения дисциплины):

- Понятие процесса.
- Понятие адресного пространства.
- Понятие файла.
- Понятие ввода-вывода.
- Понятие шины.
- Системные вызовы.
- Монолитные системы.
- Микроядра.
- Виртуальные машины.
- Модель процесса.
- Состояние процессов.
- Моделирование режима многозадачности.
- Потоки в POSIX.
- Реализация потоков в пользовательском пространстве,
- Реализация потоков в ядре.
- Гибридная реализация потоков.
- Алгоритм активации планировщика.
- Состязательные ситуации.
- Критические области.
- Синхронизационные примитивы.
- Семафор.
- Мьютекс.
- Монитор.
- Барьеры.
- Передача сообщений.
- Планирование в пакетных системах.
- Планирование в интерактивных системах.
- Планирование в системах реального времени.
- Планирование потоков.
- Классические задачи взаимодействия процессов.
- Виртуальная память.
- Страничная организация памяти.
- Алгоритмы замещения страниц.
- Алгоритм LRU.
- Алгоритм WSClock.
- Алгоритм "рабочий набор".
- Управление загрузкой.
- Разделение пространства команд и данных.
- Совместно используемые страницы и библиотеки.
- Политика очистки страниц.
- Интерфейс виртуальной памяти.
- Сегментация со страничной организацией памяти.
- Файловые системы. Свойства файлов.
- Файловые системы с журнальной структурой.
- Журналируемые файловые системы.
- Виртуальные файловые системы.
- Непротиворечивость ФС.
- Оценка производительности ФС.
- Устройства и контроллеры устройств ввода-вывода.

- Ввод-вывод, отображаемый на адресное пространство.
- Прямой доступ к памяти.
- ПО ввода-вывода.
- Ввод-вывод, управляемый прерываниями.
- Ввод-вывод с помощью DMA.
- Обработчики прерываний, драйверы устройств.
- Слой абстракции от оборудования (HAL).
- Аппаратная часть дисков.
- Алгоритмы планирования перемещения блока головок.
- Обработка ошибок при обращении к жесткому диску.
- Аппаратная составляющая часов. Программируемые таймеры.
- Пользовательский интерфейс ввода-вывода - клавиатура, мышь, монитор.
- Управление энергопотреблением.
- Выгружаемые и невыгружаемые ресурсы.
- Условия возникновения ресурсных взаимоблокировок.
- Обнаружение взаимоблокировок разных типов.
- Уклонение от взаимоблокировок, алгоритм банкира.
- Атака условия взаимного исключения.
- Атака условия удержания и ожидания.
- Атака условия невыгружаемости.
- Атака условия циклического ожидания.
- Двухфазное блокирование. Активная взаимоблокировка. Зависание.
- Технологии виртуализации. Гипервизоры первого и второго типа.
- Аппаратная поддержка вложенных таблиц страниц. Возвращение памяти.
- Виртуализация ввода-вывода.
- Блоки управления памятью при вводе-выводе.
- Домены устройств.
- Виртуальные машины на мультиядерных центральных процессорах.
- Облака в качестве услуги.
- Виртуализация на примере продуктов VmWare.
- Многопроцессорные системы.
- Коммуникационные программы мультикомпьютеров.
- Распределенная совместно используемая память.
- Планирование мультикомпьютеров.
- Вызовы удаленных процедур.
- Балансировка нагрузки.
- Реализация формальных моделей безопасности в операционных системах.
- Реализация криптографических схем в ОС.
- Криптопроцессоры и криптопровайдеры.
- Аутентификация и авторизация в современных операционных системах.
- Атаки переполнения буфера.
- Атаки, использующие форматирующую строку.
- Указатели на несуществующие объекты.
- Разыменование нулевого указателя.
- Переполнение целочисленных значений.
- Атаки, использующие внедрение команд.
- Инсайдерские атаки.
- Вредоносные программы.
- Брандмауэры.
- Антивирусные технологии.
- Электронная подпись программ.

- Защита кода типа "Тюремное заключение".
- Обнаружение проникновения на основе модели.
- Инкапсулированный код.

Вопросы и задания для самостоятельной работы студентов:

1. Механизмы управления памятью в ОС Windows
2. Организация системных вызовов ОС Windows
3. Структура ядра операционной системы Windows
4. Механизмы управления памятью в ОС Linux
5. Организация системных вызовов ОС Linux
6. Структура ядра операционной системы Linux
7. Контексты безопасности SELinux
8. Механизмы Data Execution Prevention (DEP)
9. Рандомизация пространства адресов (ASLR)
10. Инкапсуляция кода в мобильных операционных системах
11. APT-угрозы и защита от них в современных операционных системах
12. EFI и системы доверенной загрузки.

Перечень тем лабораторных работ: (Каждая лабораторная работа рассчитана на 4 часа)

Лабораторная работа №1. Создание многопоточного приложения для обмена текстовыми сообщениями. Проектирование клиент-серверной архитектуры приложения.

Лабораторная работа №2. Создание многопоточного приложения для обмена текстовыми сообщениями. Разработка потоков, реализующих доступ к базе данных, пользовательский ввод-вывод, доступ к сокетам и сетевым интерфейсам.

Лабораторная работа №3. Создание многопоточного приложения для обмена текстовыми сообщениями. Синхронизация потоков, разработка необходимых примитивов синхронизации, задействование моделей "произвдитель-потребитель". Реализация обмена информацией между потоками на базе синхронизированных структур данных.

Лабораторная работа №4. Создание многопоточного приложения для обмена текстовыми сообщениями. Защита клиента и сервера от копирования. Реализация статической защиты (от обратной разработки), динамической защиты (от отладки) и контроля целостности для предотвращения несанкционированной модификации исполняемых файлов.

Лабораторная работа №5. Создание многопоточного приложения для обмена текстовыми сообщениями. Тестирование, отладка. Упаковка приложения в дистрибутив. Нагрузочное тестирование приложения.

Лабораторная работа №6. Анализ защищенности приложения. Знакомство со средой дизассемблирования. Статический анализ кода. Анализ строк и системных вызовов. Обнаружение упаковщика и шифратора кода.

Лабораторная работа №7. Анализ защищенности приложения. Динамический анализ и отладка. Мониторинг памяти. Деобфускация кода

Лабораторная работа №8. Анализ защищенности приложения. Способы обхода механизмов контроля целостности. Обнаружение и подмена имитовставок, контрольных сумм, хэш-сумм.

Лабораторная работа №9. Анализ защищенности приложения. Тестирование на защиту от атак типа "отказ в обслуживании", атак, подразумевающих удаленное исполнение кода и атак, заключающихся в динамической подмене библиотек.

Перечень тем и заданий к курсовой работе:

Курсовая работа разделяется на две части: разработку приложения для обмена текстовыми сообщениями по сетям TCP/IP в защищенном исполнении и анализ защищенности этого приложения индивидуально по вариантам. В ходе разработки студент имеет право выбирать язык разработки и средства защиты из перечня предварительно им изученных (например, в ходе изучения дисциплины "Языки программирования").

Работу можно разбить на ряд этапов: - проектирование клиент-серверной архитектуры приложения; - разработка потоков, реализующих доступ к базе данных, пользовательский

ввод-вывод, доступ к сокетам и сетевым интерфейсам; - реализация обмена информацией между потоками на базе синхронизированных структур данных; - реализация статической защиты, динамической защиты и контроля целостности; - тестирование и отладка; - статический анализ кода; - динамический анализ и отладка с целью обхода защиты; - тестирование на возможность обхода механизмов контроля целостности.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Основная литература:

1. Операционные системы, среды и оболочки: Учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2013. - 560 с. ISBN 978-5-91134-743-7, Режим доступа: http://znanium.com/catalog.php?bookinfo=405821

2. Операционные системы. Основы UNIX: Учебное пособие/Вавренюк А.Б., Курышева О.К., Кутепов С.В. и др. - М.: НИЦ ИНФРА-М, 2015. - 184 с.: ISBN 978-5-16-010893-3, Режим доступа: http://znanium.com/catalog.php?bookinfo=504874

3. Башлы, П. Н. Информационная безопасность и защита информации: Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2 Режим доступа: http://znanium.com/catalog.php?bookinfo=405000

б) Дополнительная литература:

1. Назаров, С. В. Операционные среды, системы и оболочки. Основы структурной и функциональной организации: Учеб. пособие / С. В. Назаров. - М.: КУДИЦ-ПРЕСС, 2007. - 504 с. ISBN 978-5-91136-036-8 Режим доступа: http://znanium.com/catalog.php?bookinfo=369379

2. Таненбаум, Эндрю. Современные операционные системы -Modern operating systems : пер. с англ. / Э. Таненбаум .— 2-е изд. — Санкт-Петербург : Питер, 2007 .— 1037 с. ISBN 5-318-00299-4 ISBN 978-5-318-00299-1.

3. Операционные системы. Основы UNIX: Учебное пособие/ ВавренюкА.Б., КурышеваО.К., КутеповС.В. и др. - М.: НИЦ ИНФРА-М, 2015. - 184 с.: ISBN 978-5-16-010893-3. Режим доступа: http://znanium.com/catalog.php?bookinfo=504874

в) Периодические издания:

1. Журнал «Вопросы защиты информации». Режим доступа: http://i-vimi.ru/editions/detail.php?SECTION_ID=155/;
2. Журнал "Information Security/Информационная безопасность". Режим доступа: http://www.itsec.ru/insec-about.php.
3. Ежемесячный теоретический и прикладной научно-технический журнал «Информационные технологии». Режим доступа http://novtex.ru/IT/.

г) Программное обеспечение и Интернет-ресурсы:

1. Образовательный сервер кафедры ИЗИ.– Режим доступа: http://edu.izi.vlsu.ru
2. Информационная образовательная сеть.- Режим доступа: http://ien.izi.vlsu.ru
3. Внутривузовские издания ВлГУ.– Режим доступа: http://e.lib.vlsu.ru/
4. ИНТУИТ. Национальный открытый университет.– Режим доступа: http://www.intuit.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

ауд. 408-2, Лекционная аудитория, количество студенческих мест – 50, площадь 60 м2, оснащение: мультимедийное оборудование (интерактивная доска Hitachi FX-77WD, проектор BenQ MX 503 DLP 2700ANSI XGA), ноутбук Lenovo Idea Pad B5045

ауд. 427а-2, лаборатория сетевых технологий, количество студенческих мест – 14, площадь 36 м2, оснащение: компьютерный класс с 8 рабочими станциями Core 2 Duo E8400 с выходом в Internet, 3 маршрутизатора Cisco 2800 Series, 6 маршрутизаторов Cisco 2621, 6 коммутаторов Cisco Catalyst 2960 Series, 3 коммутатора Cisco Catalyst 2950 Series, коммутатор Cisco Catalyst Express 500 Series, проектор BenQ MP 620 P, экран настенный рулонный. Лицензионное программное обеспечение: операционная система Windows 7 Профессиональная, офисный пакет приложений Microsoft Office Профессиональный плюс 2007, бесплатно распространяемое программное обеспечение: линейка интегрированных сред разработки Visual Studio Express 2012, программный продукт виртуализации Oracle VM VirtualBox 5.0.4, симулятор сети передачи данных Cisco Packet Tracer 7.0, интегрированная среда разработки программного обеспечения IntelliJ IDEA Community Edition 15.0.3.

ауд. 427б-2, УНЦ «Комплексная защита объектов информатизации», количество студенческих мест – 15, площадь 52 м2, оснащение: компьютерный класс с 7 рабочими станциями Alliance Optima P4 с выходом в Internet, коммутатор D-Link DGS-1100-16 мультимедийный комплект (проектор Toshiba TLP X200, экран настенный рулонный), прибор ST-031P «Пиранья-Р» многофункциональный поисковый, прибор «Улан-2» поисковый, виброакустический генератор шума «Соната АВ 1М», имитатор работы средств нелегального съема информации, работающих по радиоканалу «Шиповник», анализатор спектра «GoodWill GSP-827», индикатор поля «SEL SP-75 Black Hunter», устройство блокирования работы систем мобильной связи «Мозайка-3», устройство защиты телефонных переговоров от прослушивания «Прокруст 2000», диктофон Edic MINI Hunter, локатор «Родник-2К» нелинейный, комплекс проведения акустических и виброакустических измерений «Спрут мини-А», видеорегистратор цифровой Best DVR-405, генератор Шума «Гном-3»,учебно-исследовательский комплекс «Сверхширокополосные беспроводные сенсорные сети» (Nano Xaos), сканирующий приемник «Icom IC-R1500», анализатор сетей Wi-Fi Fluke AirCheck с активной антенной. Лицензионное программное обеспечение: Windows 8 Профессиональная, офисный пакет приложений Microsoft Office Профессиональный плюс 2010, бесплатно распространяемое программное обеспечение: линейка интегрированных сред разработки Visual Studio Express 2012, инструмент имитационного моделирования AnyLogic 7.2.0 Personal Learning Edition, интегрированная среда разработки программного обеспечения IntelliJ IDEA Community Edition 14.1.4.

Программа составлена в соответствии с требованиями ФГОС ВО по специальности 10.05.04 "Информационно-аналитические системы безопасности", специализация «автоматизация информационно-аналитической деятельности»

Рабочую программу составил доцент кафедры ИЗИ к.т.н. Монахов Ю.М.
(ФИО, подпись)

Рецензент
(представитель работодателя) Заместитель руководителя РАЦ ООО «ИнфоЦентр»
к.т.н. Вертилевский Н.В.
(место работы, должность, ФИО, подпись)

Программа рассмотрена и одобрена на заседании кафедры ИЗИ
Протокол № 7 от 28.12.16 года
Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии по специальности 10.05.04 «Информационно-аналитические системы безопасности».
Протокол № 4 от 28.12.16 года
Председатель комиссии д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)

Рабочая программа одобрена на 2017/18 учебный год
Протокол заседания кафедры № 1 от 28.08.17 года
Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)

Рабочая программа одобрена на _____ учебный год
Протокол заседания кафедры № _____ от _____ года
Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)

Приложение

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)

Институт _____

Кафедра _____

Актуализированная
рабочая программа
рассмотрена и одобрена
на заседании кафедры
протокол № ____ от ____ 20__ г.

Заведующий кафедрой

_____
(подпись, ФИО)

Актуализация рабочей программы дисциплины

_____
(наименование дисциплины)

Направление подготовки

Профиль/программа подготовки

Уровень высшего образования

Форма обучения

Владимир 20__

Рабочая программа учебной дисциплины актуализирована в части рекомендуемой литературы.

Актуализация выполнена: _____

(подпись, должность, ФИО)

а) основная литература: _____

б) дополнительная литература: _____

в) периодические издания: _____

в) интернет-ресурсы: _____