

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сахалинский государственный университет»

Кафедра информатики

УТВЕРЖДЕН
на заседании кафедры
«19» марта 2024 г., протокол № 8
Исполняющий обязанности
заведующего кафедрой



Осипов Г.С.

**ФОНД
ОЦЕНОЧНЫХ СРЕДСТВ
ПО ДИСЦИПЛИНЕ (МОДУЛЮ)**

Б1.В.ДВ.05.01 Анализ уязвимостей ПО

Направление подготовки
10.03.01 Информационная безопасность
профиль

Безопасность автоматизированных систем (по отрасли или в сфере профессиональной
деятельности)

Уровень высшего образования
БАКАЛАВРИАТ

Южно-Сахалинск
2024 г.

1. Формируемые компетенции и индикаторы их достижения по дисциплине (модулю)

Код компетенции	Содержание компетенции	Код и наименование индикатора достижения компетенции
ПКС-1	Способен проводить формализацию предметной области с целью создания информационной системы в сфере профессиональной деятельности	ПКС-1.1 - Знает критерии оценки эффективности и надежности средств защиты программного обеспечения автоматизированных систем; ПКС-1.2 - Умеет определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы; ПКС-1.3 – Владеет навыками определения параметров настройки программного обеспечения системы защиты информации автоматизированной системы;
ПКС-2	Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	ПКС-2.1 - Знает основные меры по защите информации в автоматизированных системах; ПКС-2.2 - Умеет регистрировать и анализировать события, связанные с защитой информации в автоматизированных системах. Умеет регистрировать и анализировать события, связанные с защитой информации в автоматизированных системах; ПКС-2.3 - Владеет навыками использования типовых программных средства резервирования и восстановления информации в автоматизированных системах.

2. Паспорт фонда оценочных средств по дисциплине (модулю)

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1 семестр			
1.	Тема 1. Предпосылки внедрения программных закладок	ПКС-1, ПКС-2	Задания к лабораторным работам, контрольные вопросы, вопросы к коллоквиуму, вопросы к экзамену
2.	Тема 2. Эволюция угроз.	ПКС-1, ПКС-2	Задания к лабораторным работам, контрольные вопросы, вопросы к коллоквиуму, вопросы к экзамену
3.	Тема 3. Основные уязвимости	ПКС-1, ПКС-2	Задания к лабораторным работам, контрольные вопросы, вопросы к коллоквиуму, вопросы к экзамену
4.	Тема 4. Целевые атаки	ПКС-1, ПКС-2	Задания к лабораторным работам, контрольные вопросы, вопросы к коллоквиуму, вопросы к экзамену
5.	Тема 5. Атаки финансовых объектов	ПКС-1, ПКС-2	Задания к лабораторным работам, контрольные вопросы, вопросы к коллоквиуму, вопросы к экзамену
6.	коллоквиумы	ПКС-1, ПКС-2	контрольные вопросы, вопросы к коллоквиуму
7.	экзамен	ПКС-1, ПКС-2	контрольные вопросы, вопросы к коллоквиуму, вопросы к экзамену

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

- освоение основных методов анализа уязвимостей программных реализаций на практике;
- освоение принципов работы с современными дизассемблерами и отладчиками;

– получение навыков устранения уязвимостей программных реализаций на компьютерных системах

Лабораторное занятие №1 (10 ч.)

Тема Поиск уязвимостей в программной реализации

Цель: освоение основных приемов и методов поиска уязвимостей в программных реализациях.

Содержание работы: анализ программных реализаций для ОС семейства Windows на предмет наличия наиболее известных уязвимостей методом экспериментов с “черным ящиком”, статическим и динамическим методами анализа программных реализаций.

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.

Лабораторное занятие №2 (10 ч.)

Тема Программные закладки

Цель: освоение основных приемов и методов создания программных закладок и противодействия программным закладкам.

Содержание работы: методы создания программной закладки, внедрения программной закладки, выявления программной закладки, удаления программной закладки.

Результат: программная закладка и программа для удаления программной закладки, 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.

Лабораторное занятие №3 (10 ч.)

Тема Атаки на компьютерную систему

Цель: освоение основных приемов и методов использования уязвимостей в компьютерной системе для атаки и организация противодействия атаке на компьютерную систему.

Содержание работы: основные уязвимости компьютерной системы, использование уязвимостей компьютерной системы для атаки, методы противодействия атаке на компьютерную систему.

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.

Форма контроля	За одну работу		Всего	
	Мин. баллов	Макс. баллов	Мин. баллов	Макс. баллов
Текущий контроль:				
Активная работа на занятии	0,25	0,5	9	18
Выполнение домашнего задания	0,75	0,75	27	27
Выполнение заданий самостоятельной работы	1	3	1	3
коллоквиум	1	3	3	9
Промежуточная аттестация (экзамен)			20	43
Итого за семестр			60	100

Примерные вопросы к зачету

1. Эволюция вирусов. Наиболее опасные вирусы
2. Как реализуются атаки переполнения буфера? Как этого избежать? Приведите пример реализации атаки.
3. Как устроены и какие бывают DoS-атаки?
4. Как организована атака MAC-flooding?
1. Что такое Phishing-сайт?
2. Как происходит подмена субдомена DNS? Сокращения названий субдоменов DNS.
3. Что такое Potentially Unwanted Program (PUP - потенциально нежелательная программа)?
4. Как атакуют WEB-серверы? Какие существуют способы встраивания вредоносного кода на страницу?
5. Что такое «Атаки нулевого дня». Что делают разработчики, узнав о таких атаках? Как узнать, что обнаружена уязвимость и как её закрыть?
6. Что такое Adware (Madware) и Grayware?
7. Как реализуются Hijackers –атаки?
8. Что такое Ransomware, Scareware и Rouge Security (rogueware)?
9. Какие виды Cross-Site Scripting (XSS) вам известны? Как они реализуются и как от них защититься?
10. Как происходит взлом WEB-приложений с помощью "отравленных" Cookie?
11. Email bombing
12. Кликеры Clickjacking и likejacking, что это?
13. Угрозы на стороне сервера. SQL Injection (SQLi).
14. Что такое ARP-spoofing и фальсификация межсайтовых запросов CSRF.
15. Как использовать черные ходы в медиа-файлах?
16. Разновидности атаки «Человек посередине (Man-In-The-Middle).»
17. Какие на данный момент актуальны атаки финансовых объектов?
18. Какие имеются скрытые угрозы безопасности?
19. Что понимают под несанкционированным доступом в машины, отключенные от Интернет?

Критерии оценки:

Оценка «зачтено» выставляется:

- студенту глубоко и прочно усвоившему программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагающему, в ответе которого увязывается теория с практикой, он показывает знакомство с литературой, правильно обосновывает и использует рациональные и современные средства решения поставленной проблемы.
- студенту, твердо знающему программный материал, грамотно и по существу, излагающему его, который не допускает существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении поставленной задачи.
- студенту, который знает только основной программный материал, но не усвоил особенностей, допускает в ответе неточности, некорректно формулирует основные законы и правила, затрудняется в выполнении практических задач.

Оценка «не зачтено» выставляется студенту, который не знает значительной части программного материала, допускает в ответе существенные ошибки, с затруднениями выполняет практические задания.

Составитель _____

Н. Ваиц
(подпись)

Вашакидзе Н.С

«13» марта 2024 г.