Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования «Новосибирский национальный исследовательский
государственный университет» (Новосибирский государственный университет, НГУ)

Факультет информационных технологий

СОГЛАСОВАНО
Декан ФИТ НГУ
_____ М.М. Лаврентьев
«23» июля 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Практическая информационная безопасность

Направление подготовки: 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА
Направленность (профиль): Компьютерные науки и системотехника

Форма обучения: очная
Год обучения: 3, семестр: 5, 6

№	Вид деятельности	Семестр	
		5	6
1	Лекции, час.		
2	Практические занятия, час.	64	64
3	Лабораторные занятия, час.		
4	Занятий в контактной форме без учета промежуточной аттестации, час, из них	64	64
5	в электронной форме, час.		
6	из них аудиторных занятий, час.	64	64
7	из них в активной и интерактивной форме, час.		
8	консультаций, час.		
9	Самостоятельная работа, час.	42	42
10	в том числе на выполнение письменных работ, час		
11	Форма аттестации (экзамен, зачет, дифференцированный зачет), час	З 2	З 2
12	Всего зачетных единиц[1]	3	3

Новосибирск 2020

[1] С учетом выделенных часов на промежуточную аттестацию

Рабочая программа дисциплины составлена на основании федерального государственного образовательного стандарта (ФГОС) высшего образования - бакалавриат по направлению подготовки 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА.

Федеральный государственный образовательный стандарт (ФГОС) высшего образования - бакалавриат по направлению подготовки 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА введен в действие приказом Минобрнауки от 19.09.2017 № 929.

Место дисциплины в структуре учебного плана: Блок ФТД Факультативы, факультативная дисциплина.

Рабочая программа дисциплины утверждена решением Ученого совета факультета информационных технологий от 22.07.2020, протокол № 77.

Программу разработал:

ассистент кафедры Компьютерных систем ФИТ — Р.К. Лебедев

Заведующий кафедрой Компьютерных систем ФИТ,
кандидат технических наук — Б.Н. Пищик

Ответственный за образовательную программу:

доцент кафедры систем информатики ФИТ,
кандидат физико-математических наук — Д.С. Мигинский

Аннотация к рабочей программе дисциплины
«Практическая информационная безопасность»

Дисциплина «Практическая информационная безопасность» реализуется в рамках образовательной программы высшего образования – программы бакалавриата 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА, направленность (профиль): КОМПЬЮТЕРНЫЕ НАУКИ И СИСТЕМОТЕХНИКА по очной форме обучения на русском языке.

Место в образовательной программе: Дисциплина «Практическая информационная безопасность» развивает знания, умения и навыки, сформированные у обучающихся по результатам изучения следующих дисциплин: «Декларативное программирование» и «Императивное программирование».

Дисциплина «Практическая информационная безопасность» реализуется в 5, 6 семестрах в рамках дисциплин (модулей) Блока ФТД Факультативы и является факультативной дисциплиной.

Дисциплина «Практическая информационная безопасность» направлена на формирование компетенций

Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-3), в части следующих индикаторов достижения компетенции:

ОПК-3.1 Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

ОПК-3.2 Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

ОПК-3.3 Владеть: навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.

Перечень основных разделов дисциплины:

Основы использования Linux и командного интерпретатора Bash, сетевые протоколы, основы криптографии, элементы архитектуры, уязвимости программ.

При освоении дисциплины студенты выполняют следующие виды учебной работы: практические занятия, самостоятельная работа.

Самостоятельная работа включает: подготовку к практическим занятиям по разделам дисциплины.

Общий объем дисциплины – 6 зачетных единиц (216 часов).

Правила аттестации по дисциплине. Текущий контроль по дисциплине «Практическая информационная безопасность» осуществляется на практических занятиях и заключается в проверке выполнения заданий по основным темам дисциплины.

Промежуточная аттестация по дисциплине «Практическая информационная безопасность» проводится по завершению каждого периода ее освоения (семестра).

Промежуточная аттестация по дисциплине проводится в два этапа:

1) Портфолио по результатам работы в семестре, включающее как минимум два задания по каждой из тем дисциплины
2) Устный зачет, состоящий из двух вопросов по темам курса. Во время ответа обучающемуся могут быть заданы дополнительные вопросы по темам дисциплины.

По результатам аттестации выставляется оценка «зачтено» или «не зачтено».

Учебно-методическое обеспечение дисциплины.

Учебно-методический комплекс по дисциплине «Практическая информационная безопасность» размещен на сайте https://n0n3m4.ru/course/

1. Внешние требования к дисциплине

Таблица 1.1

Компетенция ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности, *в части следующих индикаторов достижения компетенции:*
ОПК-3.1 Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
ОПК-3.2 Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
ОПК-3.3 Владеть: навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.

2. Требования к результатам освоения дисциплины

Таблица 2.1

Результаты изучения дисциплины по уровням освоения (иметь представление, знать, уметь, владеть)	**Формы организации занятий**	
	Практические работы	**Самостоятельная работа**
ОПК-3.1 Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.		
1. Знать основные угрозы информационной безопасности	+	+
ОПК-3.2 Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.		
2. Знать основные методы обнаружения проблем информационной безопасности	+	+
3. Уметь обнаруживать и исправлять типичные уязвимости в программном обеспечении	+	+
ОПК-3.3 Владеть: навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности		
4. Знать основные методы эксплуатации уязвимостей в программном обеспечении	+	+
5. Уметь эксплуатировать уязвимости в программном обеспечении и определять их уровень угрозы	+	+

3. Содержание и структура учебной дисциплины

Таблица 3.1

Темы практических занятий	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 5				
Тема 1. Основы использования Linux и командного интерпретатора Bash	0	4	1	Выполнение заданий на учебном сервере
Тема 2. Протоколы IP, TCP, UDP. Протокол DNS. Классические атаки	0	4	1,2	Выполнение заданий на учебном сервере
Тема 3. Протокол HTTP, методы, URL-кодирование. Уязвимости раскрытия информации (robots.txt, .git, .svn)	0	8	1,2,3,4,5	Выполнение заданий на учебном сервере
Тема 4. Уязвимости типа "инъекции". Основы SQL, SQL-инъекции и их виды	0	8	1,2,3,4,5	Выполнение заданий на учебном сервере
Тема 5. Инъекции команд, NoSQL-инъекции, инъекции шаблонов	0	4	1,2,3,4,5	Выполнение заданий на учебном сервере
Тема 6. Path traversal, LFI.	0	4	1,2,3,4,5	Выполнение заданий на учебном сервере
Тема 7. Межсайтовый скриптинг (XSS), инъекции в HTTP-заголовки, атаки типа Open Redirect	0	4	1,2,3,4,5	Выполнение заданий на учебном сервере
Тема 8. История криптографии (криптография античности, шифры Цезаря, шифры замены, шифр Виженера, Скитала и др.)	0	4	1,2,3,4,5	Выполнение заданий на учебном сервере
Тема 9. Методы кодирования информации (двоичное кодирование, base64, шестнадцатеричное кодирование, код Морзе, кодировки ASCII и UTF)	0	4	1,2,3,4,5	Выполнение заданий на учебном сервере
Тема 10. Обзор методов симметричной криптографии (блочные и поточные шифры, генераторы псевдослучайных чисел, атаки на ГПСЧ, padding oracle, CBC)	0	8	1,2,3,4,5	Выполнение заданий на учебном сервере
Тема 11. Обзор методов асимметричной криптографии (RSA, основы эллиптической криптографии, классические атаки на RSA)	0	8	1,2,3,4,5	Выполнение заданий на учебном сервере
Тема 12. Криптографические хэш-функции (MD5, SHA, атака удлинения сообщения, способы генерации коллизий второго рода)	0	4	1,2,3,4,5	Выполнение заданий на учебном сервере
Итого за семестр 5		**64**		
Семестр: 6				
Тема 1. Виды процессорных	0	8	1	Выполнение заданий

архитектур, основные архитектуры: x86, ARM. Процессорные инструкции и машинный код. Ассемблер.				на учебном сервере
Тема 2. Краткий обзор инструкций x86. Регистры и стек. Соглашения о вызовах функций. Системные вызовы.	0	8	1,2	Выполнение заданий на учебном сервере
Тема 3. Форматы исполняемых файлов PE и ELF. Секции и сегменты, разрешения страниц памяти.	0	4	1,2	Выполнение заданий на учебном сервере
Тема 4. Обзор существующих дизассемблеров и отладчиков. Отладка.	0	4	1,2,3,4,5	Выполнение заданий на учебном сервере
Тема 5. Пакеры и протекторы, механизмы обфускации машинного кода.	0	4	1,2,3,4,5	Выполнение заданий на учебном сервере
Тема 6. Инструменты автоматизации обратной разработки. Angr, Z3.	0	4	1,2,3,4,5	Выполнение заданий на учебном сервере
Тема 7. Обзор обратной разработки байткода виртуальных машин: Java, .NET, Python.	0	4	1,2,3,4,5	Выполнение заданий на учебном сервере
Тема 8. Обзор двоичных уязвимостей программ. Уязвимости типа "отказ в обслуживании". Инструменты для автоматического поиска таких уязвимостей (фуззеры).	0	4	1,2,3,4,5	Выполнение заданий на учебном сервере
Тема 9. Шеллкод. Переполнение буфера на стеке. Перехват потока исполнения программы.	0	8	1,2,3,4,5	Выполнение заданий на учебном сервере
Тема 10. Методы защиты от переполнений. PIE, Stack canary, неисполняемый стек. Атака возврата в библиотеку, ROP.	0	4	1,2,3,4,5	Выполнение заданий на учебном сервере
Тема 11. Уязвимости форматной строки.	0	4	1,2,3,4,5	Выполнение заданий на учебном сервере
Тема 12. Переполнение буфера на куче. Use-after-free.	0	8	1,2,3,4,5	Выполнение заданий на учебном сервере
Итого за семестр 6		**64**		

4. Самостоятельная работа студентов

Таблица 4.1

№	Виды самостоятельной работы	Ссылки на результаты обучения	Часы на выполнение	Часы на консультации
Семестр: 5				
1	Подготовка к практическим занятиям.	1,2,3,4,5	38	0
	Обучающиеся самостоятельно изучают статьи по темам практических занятий. Методические рекомендации по подготовке к занятиям представлены в учебно-методическом комплексе дисциплины.			
2	Подготовка к зачету	1,2,3,4,5	4	0

	Подготовка к зачету по вопросам, представленным в фонде оценочных средств, являющихся приложением к рабочей программе дисциплины.			
Итого за семестр 5			**42**	0
Семестр: 6				
3	Подготовка к практическим занятиям.	1,2,3,4,5	38	0
	Обучающиеся самостоятельно изучают статьи по темам практических занятий. Методические рекомендации по подготовке к занятиям представлены в учебно-методическом комплексе дисциплины.			
4	Подготовка к зачету	1,2,3,4,5	4	0
	Подготовка к зачету по вопросам, представленным в фонде оценочных средств, являющихся приложением к рабочей программе дисциплины.			
Итого за семестр 6			**42**	0

5. Образовательные технологии

В ходе реализации учебного процесса по дисциплине проводятся практические занятия. Темы, изучаемые самостоятельно, закрепляются путем выполнения практических заданий, по вопросам, вызывающим затруднения, проводятся консультации.

В ходе реализации учебного процесса по дисциплине применяются следующие интерактивные формы организации учебных занятий (таблица 5.1).

Таблица 5.1

1	Портфолио	ОПК-3
Формируемые умения: 3. Уметь обнаруживать и исправлять типичные уязвимости в программном обеспечении. 5. Уметь эксплуатировать уязвимости в программном обеспечении и определять их уровень угрозы.		
Краткое описание применения: студенты ведут портфолио в системе CTFd, которое является основой для проведения аттестации по дисциплине.		

Для организации и контроля самостоятельной работы студентов, а также проведения консультаций применяются информационно-коммуникационные технологии. (таблица 5.2).

Таблица 5.2

Информирование	Почтовый адрес n0n3m4@gmail.com, конференция в системе мгновенного обмена сообщениями
Консультирование	Почтовый адрес n0n3m4@gmail.com, конференция в системе мгновенного обмена сообщениями
Контроль	Система проверки заданий CTFd
Размещение учебных материалов	Сайт https://n0n3m4.ru/course/

6. Правила аттестации студентов по учебной дисциплине

По дисциплине «Практическая информационная безопасность» проводится текущая и промежуточная аттестация (итоговая по дисциплине).

Текущая аттестация по дисциплине «Практическая информационная безопасность» осуществляется на практических занятиях и заключается в проверке выполнения заданий. По результатам текущей аттестации выставляется оценка «зачтено» или «не зачтено». Количество выполненных заданий является основным условием успешного прохождения промежуточной аттестации.

Для получения оценки «зачтено» должно быть решено как минимум два задания по каждой из тем дисциплины.

Промежуточная аттестация (итоговая по дисциплине) проводится по завершению каждого периода ее освоения (семестра) в форме зачета, а также на основании портфолио. Для получения оценки «зачтено» должно быть решено как минимум два задания по каждой из тем дисциплины.

По результатам освоения дисциплины «Практическая информационная безопасность» выставляется оценка «зачтено» или «не зачтено».

В таблице 6.1 представлено соответствие форм аттестации заявляемым требованиям к результатам освоения дисциплины.

Таблица 6.1

Коды компетенций	**Результаты обучения**	**Формы аттестации**			
		Семестр 5		**Семестр 6**	
		Портфолио	**Зачет**	**Портфолио**	**Зачет**
ОПК.3	**ОПК-3.1** Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.		+		+
ОПК.3	**ОПК-3.2** Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	+		+	
ОПК.3	**ОПК-3.3** Владеть: навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	+		+	

Требования к структуре и содержанию портфолио, оценочные средства, а также критерии оценки сформированности компетенций и освоения дисциплины в целом, представлены в Фонде оценочных средств, являющемся приложением 1 к настоящей рабочей программе дисциплины.

7. Литература

1. Прохорова, О.В. Информационная безопасность и защита информации: учебник / О.В. Прохорова; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». - Самара: Самарский государственный архитектурно-строительный университет, 2014. - 113 с. - ISBN 978-5-9585-0603-3; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=438331

Интернет-ресурсы

Таблица 7.1

№ п/п	Наименование Интернет-ресурса	Краткое описание
1	CTF Wiki [Электронный ресурс] URL: https://ctf-wiki.github.io/ctf-wiki/index-en/	Теоретическая информация о существующих уязвимостях программного обеспечения
2	PayloadAllTheThings [Электронный ресурс] URL: https://github.com/swisskyrepo/PayloadsAllTheThings/	Описание способов эксплуатации многих видов уязвимостей в программном обеспечении
3	OWASP Cheat Sheet Series [Электронный ресурс] URL: https://cheatsheetseries.owasp.org/	Описание способов защиты от многих видов уязвимостей программного обеспечения

8. Учебно-методическое и программное обеспечение дисциплины

8.1. Учебно-методическое обеспечение

Материалы по курсу на сайте https://n0n3m4.ru/course/

8.2. Программное обеспечение

Для обеспечения реализации дисциплины используется программное обеспечение, разворачиваемое студентами в ходе практических занятий.

Специализированное ПО не требуется.

9. Профессиональные базы данных и информационные справочные системы

1. Встроенное системное руководство man (входит в состав системы Ubuntu 18.04)
2. Электронная библиотека диссертаций Российской государственной библиотеки (ЭБД РГБ)
3. Лицензионные материалы на сайте eLibrary.ru

10. Материально-техническое обеспечение

Таблица 10.1

№	Наименование	Назначение
1	Презентационное оборудование (мультимедиа-проектор, экран, компьютер для управления)	Для проведения практических занятий
2	Компьютерный класс (с выходом в Internet)	Для организации самостоятельной работы обучающихся

Материально-техническое обеспечение образовательного процесса по дисциплине для обучающихся из числа лиц с ограниченными возможностями здоровья осуществляется согласно «Порядку организации и осуществления образовательной деятельности по образовательным программам для инвалидов и лиц с ограниченными возможностями здоровья в Новосибирском государственном университете».

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования «Новосибирский национальный исследовательский
государственный университет» (Новосибирский государственный университет, НГУ)

Факультет информационных технологий

СОГЛАСОВАНО
Декан ФИТ НГУ

М.М. Лаврентьев
«23» июля 2020 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ
по дисциплине Практическая информационная безопасность

Направление подготовки: 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

Направленность (профиль): Компьютерные науки и системотехника

Квалификация: бакалавр

Форма обучения: очная Год обучения: 3 семестр 5, 6

Форма аттестации	Семестр
Зачет	5
Зачет	6

Новосибирск 2020

Фонд оценочных средств промежуточной аттестации по дисциплине является **Приложением 1** к рабочей программе дисциплины «Практическая информационная безопасность», реализуемой в рамках образовательной программы высшего образования – программы бакалавриата 09.03.01 Информатика и вычислительная техника, направленность (профиль): Компьютерные науки и системотехника.

Фонд оценочных средств промежуточной аттестации по дисциплине утвержден решением ученого совета факультета информационных технологий, протокол № 77 от 22.07.2020.

Разработчики:
ассистент кафедры Компьютерных систем ФИТ — Р.К. Лебедев

Заведующий кафедрой Компьютерных систем ФИТ,
кандидат технических наук — Б.Н. Пищик

Ответственный за образовательную программу:

доцент кафедры систем информатики ФИТ,
кандидат физико-математических наук — Д.С. Мигинский

1. Содержание и порядок проведения промежуточной аттестации по дисциплине

1.1. Общая характеристика содержания промежуточной аттестации

Промежуточная аттестация по дисциплине «Практическая информационная безопасность» проводится по завершению периода освоения образовательной программы (семестра) для оценки сформированности компетенций в части следующих индикаторов достижения компетенции (таблица П1.1).

Таблица П1.1

Код	Компетенции, формируемые в рамках модуля «Практическая информационная безопасность»	Семестр 5		Семестр 6	
		Портфолио	Зачет	Портфолио	Зачет
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности					
ОПК.3.1	**ОПК-3.1** Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.		+		+
ОПК.3.2	**ОПК-3.2** Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	+		+	
ОПК.3.3	**ОПК-3.3** Владеть: навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	+		+	

Промежуточная аттестация включает 2 этапа. Часть компетенций оценивается портфолио, в которое входят работы, выполненные в рамках дисциплины. Часть компетенций оценивается зачетом.

Тематика вопросов к зачету включает следующие разделы:

1. В 5 семестре - Основы использования Linux и командного интерпретатора Bash, Сетевые протоколы, Основы криптографии.
2. В 6 семестре - Элементы архитектуры, Уязвимости программ.

1.2. Порядок проведения промежуточной аттестации по дисциплине

Необходимым условием для прохождения промежуточной аттестации является оценка «зачтено» по результатам всех выполненных и сданных в течение семестра заданий (портфолио).

Оценка «зачтено» за выполненные задания выставляется при выполнении всех следующих условий:

1) Решено как минимум две задачи на каждую из пройденных тем.
2) В каждой из решенных задач получен правильный ответ.

Зачет проводится в устной форме. Во время проведения зачета студенту разрешается использовать справочники, калькуляторы. В процессе ответа на вопросы студенту могут быть заданы дополнительные вопросы по темам дисциплины.

2. Требования к структуре и содержанию фонда оценочных средств промежуточной аттестации по дисциплине

Перечень оценочных средств, применяемых на каждом этапе проведения промежуточной аттестации по дисциплине, представлен в таблице П1.3.

Таблица П1.3

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
Семестр 5			
Этап 1 - портфолио			
1	Портфолио	Решение задач по темам дисциплины и сдача их в систему проверки CTFd.	Комплект разноуровневых заданий
Этап 2 - зачет			
2	Собеседование	Средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п.	Вопросы по темам/разделам дисциплины
Семестр 6			
Этап 1 - портфолио			
3	Портфолио	Решение задач по темам дисциплины и сдача их в систему проверки CTFd.	Комплект разноуровневых заданий
Этап 2 - зачет			
4	Собеседование	Средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п.	Вопросы по темам/разделам дисциплины

2.1 Требования к структуре и содержанию оценочных средств аттестации

2.1.1 Требования к структуре и содержанию портфолио
Портфолио должно содержать не менее двух выполненных задач по каждой из 12 предложенных в течение каждого семестра тем. Задачи сдаются в систему тестирования CTFd.

2.1.2 Перечень вопросов для зачета:
5 семестр:

1. Основы использования Linux и командного интерпретатора Bash

2. Протоколы IP, TCP, UDP. Протокол DNS. Классические атаки
3. Протокол HTTP, методы, URL-кодирование. Уязвимости раскрытия информации (robots.txt, .git, .svn)
4. Уязвимости типа "инъекции". Основы SQL, SQL-инъекции и их виды
5. Инъекции команд, NoSQL-инъекции, инъекции шаблонов
6. Path traversal, LFI.
7. Межсайтовый скриптинг (XSS), инъекции в HTTP-заголовки, атаки типа Open Redirect
8. История криптографии (криптография античности, шифры Цезаря, шифры замены, шифр Виженера, Скитала и др.)
9. Методы кодирования информации (двоичное кодирование, base64, шестнадцатеричное кодирование, код Морзе, кодировки ASCII и UTF)
10. Обзор методов симметричной криптографии (блочные и поточные шифры, генераторы псевдослучайных чисел, атаки на ГПСЧ, padding oracle, CBC)
11. Обзор методов асимметричной криптографии (RSA, основы эллиптической криптографии, классические атаки на RSA)
12. Криптографические хэш-функции (MD5, SHA, атака удлинения сообщения, способы генерации коллизий второго рода)

6 семестр:

13. Виды процессорных архитектур, основные архитектуры: x86, ARM. Процессорные инструкции и машинный код. Ассемблер.
14. Краткий обзор инструкций x86. Регистры и стек. Соглашения о вызовах функций. Системные вызовы.
15. Форматы исполняемых файлов PE и ELF. Секции и сегменты, разрешения страниц памяти.
16. Обзор существующих дизассемблеров и отладчиков. Отладка.
17. Пакеры и протекторы, механизмы обфускации машинного кода.
18. Инструменты автоматизации обратной разработки. Angr, Z3.
19. Обзор обратной разработки байткода виртуальных машин: Java, .NET, Python.
20. Обзор двоичных уязвимостей программ. Уязвимости типа "отказ в обслуживании". Инструменты для автоматического поиска таких уязвимостей (фуззеры).
21. Шеллкод. Переполнение буфера на стеке. Перехват потока исполнения программы.
22. Методы защиты от переполнений. PIE, Stack canary, неисполняемый стек. Атака возврата в библиотеку, ROP.
23. Уязвимости форматной строки.
24. Переполнение буфера на куче. Use-after-free.

3. Критерии оценки сформированности компетенций в рамках промежуточной аттестации по дисциплине

Таблица П1.5

Шифр компетенций	Структурные элементы оценочных средств	Показатель сформированности	Не сформирован	Сформирован (пороговый уровень)
ОПК-3	Зачет	**ОПК-3.1** Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	Знание основных угроз информационной безопасности отсутствует, студент не ориентируется в базовых понятиях, допускает грубые ошибки.	Знание основных угроз информационной безопасности присутствует. Студент ориентируется в базовых понятиях дисциплины.
ОПК-3	Портфолио	**ОПК-3.2** Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	Умение отсутствует, студент не способен обнаруживать и исправлять уязвимости в программном обеспечении.	Умение присутствует, студент способен самостоятельно обнаруживать и исправлять простые уязвимости в программном обеспечении.
ОПК-3	Портфолио	**ОПК-3.3** Владеть: навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	Умение отсутствует, студент не способен эксплуатировать уязвимости в программном обеспечении.	Умение присутствует, студент способен самостоятельно эксплуатировать простые уязвимости в программном обеспечении, а также определять их уровень угрозы.

4. Критерии выставления оценок по результатам промежуточной аттестации по дисциплине

Результаты промежуточной аттестации 5 и 6 семестрах определяются оценками «зачтено» и «не зачтено». Оценка «зачтено» означает успешное прохождение промежуточной аттестации и выставляется, если компетенции сформированы на пороговом уровне. Оценка «не зачтено» означает, что дисциплина не освоена и выставляется, если хотя бы одна компетенция не сформирована.