МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования

«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

	`	УТВЕРЖДАЮ
	Проректор по у	учебной работе
		С.Т. Князев
~	»	2018 г.

РАБОЧАЯ ПРОГРАММА МОДУЛЯ ПРАКТИКУМ ПО КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Перечень сведений о рабочей программе модуля	Учетные данные
Модуль	Код модуля 1136620
Практикум по компьютерной безопасности	
	УП № 5345
Образовательная программа	Код ОП
Фундаментальная информатика и информационные тех-	02.03.02/01.02
нологии	
Траектория образовательной программы (ТОП)	Не предусмотрено
Направление подготовки	Код направления и уровня подго-
Фундаментальная информатика и информационные тех-	товки
нологии	02.03.02
Уровень подготовки	
Бакалавриат	
ΦΓΟС ΒΟ	Реквизиты приказа Минобрнауки
	РФ об утверждении ФГОС ВО:
	№ 224 от 12.03.2015

Екатеринбург, 2018

Программа модуля составлена авторами:

№ п/п	ФИО	Ученая степень, ученое звание	Должность	Кафедра	Подпись
1	Гейн Андрей	нет	инженер	РУНЦ	
	Александрович			«Информационная	
				безопасность»	

Руководитель модуля

А.М. Шур

Рекомендовано учебно-методическим советом института математики и компьютерных наук

Председатель учебно-методического совета Протокол № 5 от 18 апреля $2016 \, \Gamma$.

А.Ю. Коврижных

Согласовано:

Дирекция образовательных программ

Р.Х. Токарева

Руководитель образовательной программы (ОП), для которой реализуется модуль А.М. Шур

1. **ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ** ПРАКТИКУМ ПО КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

1.1. Объем модуля 6 з.е.

1.2. Аннотация содержания модуля

Состоит из дисциплины «Практикум по компьютерной безопасности», ориентированной практическое применение навыков обеспечения компьютерной безопасности на уровне операционной системы, сетевых протоколов и приложений.

1. СТРУКТУРА МОДУЛЯ И РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ ПО ДИСЦИПЛИНАМ

Наименования дисциплин с указанием, к какой части образовательной программы они относятся: базовой (Б), вариативной – по выбору вуза (ВВ), вариативной - по выбору студента (ВС). 1. (ВС) Практикум по компьютерной безопасности		K	Ауд	Объем			ый на освоение ;	дисциплин мод	уля Всего дисциі	-
		изучен	Лекции	Практические занятия	Лабораторные работы	Всего	Самостоя- тельная работа, включая все виды теку- щей атте- стации, час.	Промежуто чная аттестация (зачет, экзамен), час.	Hac.	Зач. ед.
		6		68		68	130	Э(18)	216	6
	Всего на освоение модул	ІЯ		68		68	130	18	216	6

2. ПОСЛЕДОВАТЕЛЬНОСТЬ ОСВОЕНИЯ ДИСЦИПЛИН В МОДУЛЕ

3.1.	Пререквизиты и постреквизиты в	-
	модуле	
3.2.	Кореквизиты	-

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ МОДУЛЯ

3.2. Планируемые результаты освоения модуля и составляющие их компетенции

Коды ОП, для которых	Планируемые в ОХОП результаты обучения -PO, которые	Компетенции в соответствии с ФГОС ВО,
реализуется	формируются при освоении мо-	а также дополнительные из ОХОП,
модуль	дуля	формируемые при освоении модуля
02.03.02/01.02	РО-ОЗ Способность использовать	ОПК-2 – способность применять в про-
	в профессиональной деятельности	фессиональной деятельности современ-
	теоретические знания и методы	ные языки программирования и языки
	современной математики, инфор-	баз данных, методологии системной ин-
	матики и информационных техно-	женерии, системы автоматизации проек-
	логий.	тирования, электронные библиотеки и
		коллекции, сетевые технологии, библио-
		теки и пакеты программ, современные
		профессиональные стандарты информа-
		ционных технологий;
		ОПК-4 – способность решать стандарт-
		ные задачи профессиональной деятель-

		voorv vo oovon1
		ности на основе информационной и биб- лиографической культуры с применением
		информационно-коммуникационных тех-
		нологий и с учетом основных требований
		информационной безопасности;
		ПК-3 – способность использовать совре-
		менные инструментальные и вычисли-
		тельные средства;
		ПК-6 - способностью эффективно приме-
		нять базовые математические знания и
		информационные технологии при реше-
		нии проектно-технических и прикладных
		задач, связанных с развитием и использо-
		l •
		ванием информационных технологий;
		ПК-8 – способность применять на прак-
		тике международные и профессиональ-
		ные стандарты информационных техно-
		логий, современные парадигмы и мето-
		дологии, инструментальные и вычисли-
		тельные средства
		ПК-10 – способность реализовывать про-
		цессы управления качеством производ-
		ственной деятельности, связанной с со-
		зданием и использованием информаци-
		онных технологий, осуществлять мони-
		торинг и оценку качества процессов про-
		изводственной деятельности.
02.03.02/01.02	РО-04 Способность самостоятель-	ОПК-3 – способность к разработке алго-
	но разрабатывать алгоритмиче-	ритмических и программных решений в
	ские, программные и проектные	области системного и прикладного про-
	решения в различных областях	граммирования, математических, инфор-
	программирования, математиче-	мационных и имитационных моделей,
	ского и информационного моде-	созданию информационных ресурсов
	_ 	глобальных сетей, образовательного кон-
	лирования.	<u> </u>
		тента, прикладных баз данных, тестов и
		средств тестирования систем и средств на
		соответствие стандартам и исходным
		требованиям;
		ПК-7 – способность разрабатывать и реа-
		лизовывать процессы жизненного цикла
		информационных систем, программного
		обеспечения, сервисов систем информа-
		ционных технологий, а также методы и
		механизмы оценки и анализа функциони-
		рования средств и систем информацион-
		ных технологий;
		ПК-11 - способность составлять и кон-
		тролировать план выполняемой работы,
		планировать необходимые для выполне-
		ния работы ресурсы, оценивать результа-
		ты собственной работы.
02.03.02/01.02	РО-В-1 Способность вести само-	ПК-2 – способность понимать, совершен-
02.03.02/01.02		
	стоятельную исследовательскую	ствовать и применять современный ма-

работу в области информатики и	тематический аппарат, фундаментальные
информационных технологий	концепции и системные методологии,
	международные и профессиональные
	стандарты в области информационных
	технологий;
	ДПК-1 – способность строить математи-
	ческие модели процессов и явлений, ана-
	лизировать модели при помощи теорети-
	ческих методов и вычислительного экс-
	перимента, формулировать гипотезы и
	доказывать строгие математические
	утверждения о моделях.

4.2.Распределение формирования компетенций по дисциплинам модуля

Дисциплины модуля		ОПК -3	ОПК -4	ПК -2	ПК -3	ПК -6	ПК -7	ПК -8	ПК -10	ПК -11	ДПК -1
(BC) Практикум по компьютерной безопасности	*	*	*	*	*	*	*	*	*	*	*

5. ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО МОДУЛЮ

Не предусмотрено

6. ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ В РАБОЧЕЙ ПРОГРАММЕ МОДУЛЯ

Номер листа изменений	Номер протокола засе- дания проектной	Дата заседания про- ектной группы	Всего листов в документе	Подпись руководителя про- ектной группы мо-
	группы модуля	модуля		дуля

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования

«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ПРАКТИКУМ ПО КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Перечень сведений о рабочей программе дисциплины	Учетные данные
Модуль	Код модуля 1136620
Практикум по компьютерной безопасности	
	УП № 5345
Образовательная программа	Код ОП
Фундаментальная информатика и информационные тех-	02.03.02/01.02
нологии	
Направление подготовки	Код направления и уровня подго-
Фундаментальная информатика и информационные тех-	товки
нологии	02.03.02
Уровень подготовки	
Бакалавриат	
ΦΓΟС ΒΟ	Реквизиты приказа Минобрнауки
	РФ об утверждении ФГОС ВО:
	№ 224 от 12.03.2015

Рабочая программа дисциплины составлена авторами:

№ п/п	ФИО	Ученая степень, ученое звание	Должность	Кафедра	Подпись
1	Гейн Андрей	нет	инженер	РУНЦ	
	Александрович			«Информационная	
				безопасность»	

Руководитель модуля

А.М. Шур

Рекомендовано учебно-методическим советом института математики и компьютерных наук

Председатель учебно-методического совета Протокол № 5 от 18 апреля 2016 г.

А.Ю.Коврижных

Согласовано:

Дирекция образовательных программ

Р.Х. Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ ПРАКТИКУМ ПО КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

1.1.Аннотация содержания дисциплины

Дисциплина «Практикум по компьютерной безопасности» составляет одноименный вариативный модуль по выбору студента. В курсе рассматривается практическое применение навыков обеспечения компьютерной безопасности на уровне операционной системы, сетевых протоколов и приложений. Студенты обучаются использовать необходимый инструментарий: средства распределения доступа, виртуализации и изоляции, снифферы трафика и другие, а также анализировать последствия компьютерных инцидентов.

1.2.Язык реализации программы - русский

1.3.Планируемые результаты освоения дисциплины

Результатом обучения в рамках дисциплины является формирование у студента следующих компетенций:

- ОПК-1 способность использовать базовые знания естественных наук, математики и информатики, основные факты, концепции, принципы теорий, связанных с фундаментальной информатикой и информационными технологиями;
- ОПК-2 способность применять в профессиональной деятельности современные языки программирования и языки баз данных, методологии системной инженерии, системы автоматизации проектирования, электронные библиотеки и коллекции, сетевые технологии, библиотеки и пакеты программ, современные профессиональные стандарты информационных технологий;
- ОПК-3 способность к разработке алгоритмических и программных решений в области системного и прикладного программирования, математических, информационных и имитационных моделей, созданию информационных ресурсов глобальных сетей, образовательного контента, прикладных баз данных, тестов и средств тестирования систем и средств на соответствие стандартам и исходным требованиям;
- ПК-1 способность собирать, обрабатывать и интерпретировать данные современных научных исследований, необходимые для формирования выводов по соответствующим научным исследованиям;
- ПК-2 способность понимать, совершенствовать и применять современный математический аппарат, фундаментальные концепции и системные методологии, международные и профессиональные стандарты в области информационных технологий:
- Π K-3 способность использовать современные инструментальные и вычислительные средства;
- ПК-6 способностью эффективно применять базовые математические знания и информационные технологии при решении проектно-технических и прикладных задач, связанных с развитием и использованием информационных технологий;
- ПК-7 способность разрабатывать и реализовывать процессы жизненного цикла информационных систем, программного обеспечения, сервисов систем информационных технологий, а также методы и механизмы оценки и анализа функционирования средств и систем информационных технологий;
- ПК-8 способность применять на практике международные и профессиональные стандарты информационных технологий, современные парадигмы и методологии, инструментальные и вычислительные средства.
- ПК-11 способность составлять и контролировать план выполняемой работы, планировать необходимые для выполнения работы ресурсы, оценивать результаты собственной работы.
- ДПК-1 способность строить математические модели процессов и явлений, анализировать модели при помощи теоретических методов и вычислительного эксперимента, формулировать гипотезы и доказывать строгие математические утверждения о моделях.

В результате освоения дисциплины студент должен:

Знать необходимые аспекты работы операционных систем, сетевых протоколов и приложений, связанных с обеспечением безопасности хранения и передачи данных.

Уметь применять теоретические знания на практике: находить уязвимости и защищать чувствительные данные от злоумышленников.

Демонстрировать навыки и опыт деятельности по практической проверке защищенности систем и поиску уязвимостей.

1.4. Объем дисциплины

		Объем ,	дисциплины	Распределение объема дисциплины по семестрам (час.)		
	Виды учебной работы	Всего ча- сов	В т.ч. кон- тактная рабо- та (час.)*	7		
1.	Аудиторные занятия	68	68	68		
2.	Лекции	0	0	0		
3.	Практические занятия	68	68	68		
4.	Лабораторные работы					
5.	Самостоятельная работа студентов, включая все виды текущей аттестации	130	10.2	130		
6.	Промежуточная аттестация	18	2.33	Э(18)		
7.	Общий объем по учебному плану, час.	216	80.53	216		
8.	Общий объем по учебному плану, з.е.	6		6		

^{*}Контактная работа составляет:

в п.5 – количество часов, равное сумме объема времени, выделенного преподавателю на консультации в группе (15% от объема аудиторных занятий) и объема времени, выделенного преподавателю на руководство курсовой работой/проектом одного студента, если она предусмотрена.

в п.6 – количество часов, равное сумме объема времени, выделенного преподавателю на проведение соответствующего вида промежуточной аттестации одного студента и объема времени, выделенного в рамках дисциплины на руководство проектом по модулю (если он предусмотрен) одного студента.

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код раздела, темы	Раздел, тема дисциплины	Содержание				
I	Бинарные уязвимости	Практикум по бинарным уязвимостям. Отладчик. GDB. Переполнение стека. Переполнение кучи. Исполнение кода, шеллкод. Уязвимость форматной строки.				
п	Соревнования СТБ	Работы с игровой виртуальной машиной, настройка сети, исследование траффика, работа с незнакомыми операционными системами, сетевыми протоколами и другими технологиями. Участие в соревнованиях. Разработка собственных заданий для соревнований				
III	Системы контейнеризации и изоляции	Работа со средствами виртуализации (VMWare, VirtualBox), контейнеризации (Docker, LXC,				

в п/п 2,3,4 - количество часов, равное объему соответствующего вида занятий;

		OpenVz) и изоляции (cgroups)
IV	Написание эксплойтов	Изучение библиотек для сетевого взаимодействия, автоматизация работы шеллкодов и backconnect-
		шеллов

3. РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ

3.1. Распределение аудиторной нагрузки и мероприятий самостоятельной работы по разделам дисциплины

Раздел дисциплины Аудиторные занятия (час.)										Сам	остоя	телы	ная р	рабо	та:	виды,	, кол	ичест	гво и	об1	ьемь	і мер			СЦИПЛИП		-H·/· -			
ā		теме (час.)	ты (час.)		ТИЯ	ОТЫ	оты студентов	-		вка к а нятия		•	Ві	ыполн	ение			оятель эт (кол		внеау	/дитс	рны	x	кон мер тек	дгото нтроль ооприя ущей гации лич.	оным ятиям атте- (ко-	Подго- проме ной ат ции п ципл (ча	жуточ- теста- о дис- пине	Подгото рамк дисципл к промиточной стации моду. (час	ах лины ежу- атте- и по лю
Код раздела, темы	Наименование раздела, темы	о по разделу,	Всего аудиторной работы	Лекции	Практические занятия	Лабораторные работы	Всего самостоятельной работы (час.)	Всего (час.)	Лекция	Практ., семинар. занятие	Лабораторное занятие	Н/и семинар, семинар-конфер., коллоквиум (магистратура)	Всего (час.)	Домашняя работа*	Графическая работа*	Реферат, эссе, творч. работа*	Проектная работа*	Расчетная работа, разработка программного продукта*	Расчетно-графическая работа*	Домашняя работа на иностр. языке*	Перевод инояз. литературы*	Курсовая работа*	Курсовой проект*	Всего (час.)	Контрольная работа*	Коллоквиум*	Зачет	Экзамен	Интегрированный экзамен по модулю	по модулю
ı	Бинарные уязвимости	57	21		21		36	21		21			15	3] "	Ō	HHP	Проект
П	Соревнования СТГ	45	15		15		30	15		15			15	3															2008	д
III	Системы контейнеризации и изоляции	28	8		8		20	8		8			12	2															1нтегри	
IV	Написание эксплой- тов	68	24		24		44	24		24			20	3																
	Всего (час), без учета проме- жуточной аттестации:	198	68		68		130	68		68	0	0	62	62	0	0	0	0	0	0	0	0	0	0	0	0				
	Всего по дисциплине (час.):	216	68				130													В т.ч	. про	меж	уточн	ая а	ттест	ация	0	18	0	0

4. ОРГАНИЗАЦИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ, САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ

4.1. Лабораторные работы

Не предусмотрено

4.2. Практические занятия

Код раздела, темы	Номер работы	Наименование работы	Время на выполнение работы (час.)		
I	1	Структура и форматы исполняемых файлов	2		
I	I 2 Обратный инжиниринг				
I	I 3 Бинарные уязвимости				
I	4	Уязвимость форматной строки	3		
II	II 5 Администрирование образа виртуальной машины		4		
II	6	Работа со сниффером трафика. Анализ трафика	4		
II	7	Поиск уязвимостей	7		
III	9	Системы виртуализации	3		
III	10	Системы контейнеризации	3		
III	11	Системы изоляции и ограничений	2		
IV	12	Написание эксплойтов	7		
IV	IV 13 Использование библиотек для сетевого взаимодействия		5		
IV	14	Backconnect-шеллы	12		
		Всего:	68		

4.3. Примерная тематика самостоятельной работы

4.3.1. Примерный перечень тем домашних работ

- 1. Бинарные уязвимости
- 2. Уязвимость форматной строки
- 3. Администрирование образа виртуальной машины
- 4. Работа со сниффером трафика. Анализ трафика
- 5. Поиск уязвимостей
- 6. Системы виртуализации
- 7. Системы контейнеризации
- 8. Системы изоляции и ограничений
- 9. Написание эксплойтов
- 10. Использование библиотек для сетевого взаимодействия
- 11. Backconnect-шеллы

4.3.2. Примерный перечень тем графических работ

не предусмотрено

4.3.3. Примерный перечень тем рефератов (эссе, творческих работ)

не предусмотрено

- **4.3.4.** Примерный перечень тем расчетных работ (программных продуктов) не предусмотрено
- 4.3.5. Примерный перечень тем расчетно-графических работ не предусмотрено
- **4.3.6.** Примерный перечень тем курсовых проектов (курсовых работ) не предусмотрено
- **4.3.7. Примерная тематика коллоквиумов** не предусмотрено

5. СООТНОШЕНИЕ РАЗДЕЛОВ ДИСЦИПЛИНЫ И ПРИМЕНЯЕМЫХ ТЕХНОЛОГИЙ ОБУЧЕНИЯ

	Aĸ	тивнь	ые мет	годы о	бучен	Дистанционные образователь- ные технологии и электронное обучение						
Код раздела, темы дисци- плины	Проектная работа	Кейс-анализ	Деловые игры	Проблемное обучение	Командная работа	Другие (указать, какие)	Сетевые учебные курсы	Виртуальные практикумы и тренажеры	Вебинары и видеоконфе- ренции	Асинхронные web- конференции и семинары	Совместная работа и разработка контента	Другие (указать, какие)
Бинарные уязвимости				*	*		*	*			*	
Соревнования СТБ				*	*		*	*			*	
Системы контейнеризации и изоляции				*	*		*	*			*	
Написание эксплойтов				*	*		*	*			*	

- 6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ (Приложение 1)
- 7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИ-СИМОГО ТЕСТОВОГО КОНТРОЛЯ (Приложение 2)
- 8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУ-ТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (Приложение 3)
- 9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ
- 9.1.Рекомендуемая литература
- 9.1.1.Основная литература
 - 1) Введение в криптографию. Под ред. В.В. Ященко. 4-е изд., доп. МНЦМО, 2012. Доступ: http://cryptography.ru/wp-content/uploads/2013/09/intro to crypto.pdf

- 2) А.К. Гультяев. Виртуальные машины. Несколько компьютеров в одном. Питер, 2006. Доступ: http://www.rulit.me/books/virtualnye-mashiny-neskolko-kompyuterov-v-odnom-read-196838-52.html
- 3) B. Schneier. Schneier on Security: Applied Cryptography Source Code. Доступ: https://www.schneier.com/books/applied cryptography/source.html

9.1.2.Дополнительная литература

- 1) Юричев Д. Reverse Engineering для начинающих. 2017. https://beginners.re/RE4B-RU.pdf
- 2) Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. М.: Гелиос АРВ, 2001. 479 с
- 3) Таненбаум Э. Современные операционные системы. СПб.: Питер, 2002

9.2. Методические разработки

не используются

9.3. Программное обеспечение

Собственная платформа для проведения практических занятий: http://training.hackerdom.ru

9.4. Базы данных, информационно-справочные и поисковые системы

http://lib.urfu.ru - Зональная научная библиотека ФГАОУ ВО УрФУ

9.5.Электронные образовательные ресурсы

Для первого раздела: записи видео-лекций с https://ulearn.me/Course/Hackerdom

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием

Не требуется

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Весовой коэффициент значимости дисциплины -

6.2. Процедуры текущей и промежуточной аттестации по дисциплине

1. Лекции: не предусмотрены										
2. Практические/семинарские занятия: коэффициент значимости совокупных результа-										
тов практических/семинарских занятий – 1										
Текущая аттестация на практических/семинарских Сроки - семестр, Максималь-										
занятиях	учебная неделя	ная оценка в								
		баллах								
Выполнение задач на занятиях	VI, 1-17	50								
СРС - выполнение домашних работ	VI, 1-17	50								
Весовой коэффициент значимости результатов текущей	аттестации по прав	ктиче-								
ским/семинарским занятиям – 0,4										
Промежуточная аттестация по практическим/семинарсн	сим занятиям – <i>экз</i>	амен								
Весовой коэффициент значимости результатов промежу	точной аттестации	по практиче-								
ским/семинарским занятиям – 0,6		_								
3. Лабораторные занятия: не предусмотрены										

6.3. Процедуры текущей и промежуточной аттестации курсовой работы - не предусмотрены

6.4. Коэффициент значимости семестровых результатов освоения дисциплины

Порядковый номер семестра по учебному пла-	Коэффициент значимости результатов
ну, в котором осваивается дисциплина	освоения дисциплины в семестре
Семестр 6	1

ПРИЛОЖЕНИЕ 2 к рабочей программе дисциплины

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте $\Phi \ni \Pi O \ \underline{http://fepo.i-exam.ru}$.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте Интернет-тренажеры http://training.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на портале CMYJC $Yp\Phi Y$.

B связи с отсутствием Дисциплины и ее аналогов, по которым возможно тестирование, на сайтах Φ ЭПО, Интернет-тренажеры и портале СМУДС Ур Φ У, тестирование в рамках НТК не проводится.

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУ-ТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

8.1. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕ-РОПРИЯТИЙ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ В РАМКАХ БРС

В рамках БРС применяются утвержденные на кафедре критерии оценивания достижений студентов по каждому контрольно-оценочному мероприятию. Система критериев оценивания, как и при проведении промежуточной аттестации по модулю, опирается на три уровня освоения компонентов компетенций: пороговый, повышенный, высокий.

компонентов компетенций: пороговый, повышенный, высокий.									
Компоненты		ия освоения компонентов	компетенций						
компетенций	Пороговый	повышенный	высокий						
Знания	Студент демонстрирует	Студент демонстрирует	Студент может само-						
	знание-знакомство, зна-	аналитические знания:	стоятельно извлекать						
	ние-копию: узнает объек-	уверенно воспроизводит	новые знания из окру-						
	ты, явления и понятия,	и понимает полученные	жающего мира, творче-						
	находит в них различия,	знания, относит их к той	ски их использовать						
	проявляет знание источ-	или иной классифика-	для принятия решений						
	ников получения инфор-	ционной группе, само-	в новых и нестандарт-						
	мации, может осуществ-	стоятельно системати-	ных ситуациях.						
	лять самостоятельно ре-	зирует их, устанавлива-							
	продуктивные действия	ет взаимосвязи между							
	над знаниями путем само-	ними, продуктивно							
	стоятельного воспроизве-	применяет в знакомых							
	дения и применения ин-	ситуациях.							
	формации.								
Умения	Студент умеет корректно	Студент умеет самосто-	Студент умеет само-						
	выполнять предписанные	ятельно выполнять дей-	стоятельно выполнять						
	действия по инструкции,	ствия (приемы, опера-	действия, связанные с						
	алгоритму в известной	ции) по решению не-	решением исследова-						
	ситуации, самостоятельно	стандартных задач, тре-	тельских задач, демон-						
	выполняет действия по	бующих выбора на ос-	стрирует творческое						
	решению типовых задач,	нове комбинации из-	использование умений						
	требующих выбора из	вестных методов, в не-	(технологий)						
	числа известных методов,	предсказуемо изменяю-							
	в предсказуемо изменяю-	щейся ситуации							
	щейся ситуации		~						
Личностные	Студент имеет низкую	Студент имеет выра-	Студент имеет разви-						
качества	мотивацию учебной дея-	женную мотивацию	тую мотивацию учеб-						
	тельности, проявляет без-	учебной деятельности,	ной и трудовой дея-						
	различное, безответствен-	демонстрирует позитив-	тельности, проявляет						
	ное отношение к учебе,	ное отношение к обуче-	настойчивость и увле-						
	порученному делу	нию и будущей трудо-	ченность, трудолюбие,						
		вой деятельности, про-	самостоятельность,						
		являет активность.	творческий подход.						

8.2. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.2.1. Примерные задания для проведения домашних работ

- 1. Найдите и проэксплуатируйте уязвимость форматной строки
- 2. Найдите и проэксплуатируйте переполнение буфера
- 3. Запустите и настройте образ виртуальной машины. Сбросьте пароль пользователя root. Обеспечьте работу локальной сети и доступ в интернет, доступ на машину по SSH.
- 4. Запустите запись всего трафика, кроме SSH. Отфильтруйте по порту сервиса. Найдите в исходящем трафике украденную приватную информацию.
- 5. Тестовая игра в СТГ-соревнование
- 6. Настройте автоматическую работу с пулом виртуальных машин на основе VMWare или Virtual Box. Должно поддерживаться автоматические создание машины с заданными параметрами, удаление, настройка машины, запуск и остановка.
- 7. Настройте работу docker-контейнеров для изоляции сервисов
- 8. Настройте ограничения указанных процессов с помощью cgroups
- 9. Напишите эксплойт с использованием библиотеки pwn
- 10. Напишите полностью автоматический эксплойт для найденной уязвимости с использованием библиотек для сетевого взаимодействия
- 11. Получите доступ к серверу через уязвимое приложение. Настройте backconnect-шелл для подключения к вашему компьютеру.

8.2.2. Перечень примерных вопросов для экзамена

- 1. Форматы исполняемых файлов.
- 2. Формат РЕ.
- 3. Шаблоны исполняемого кода.
- 4. Шаблоны объектно-ориентированного программирования.
- 5. Пакеты.
- 6. Антиотладка.
- 7. Отладчик.
- 8. GDB.
- 9. Переполнение стека.
- 10. Переполнение кучи.
- 11. Исполнение кода, шеллкод.
- 12. OpenSSL Heartbleed.
- 13. Уязвимость форматной строки.
- 14. Администрирование образа виртуальной машины
- 15. Запись сетевого трафика, фильтрация трафика
- 16. Исследование дампа трафика
- 17. Поиск уязвимостей
- 18. Написание эксплойтов
- 19. Системы контейнеризации
- 20. Системы изоляции процессов

8.2.3. Интернет-тренажеры

- 1. http://training.hackerdom.ru
- 2. https://ulearn.me/Course/Hackerdom