

**ОЦЕНОЧНЫЕ МАТЕРИАЛЫ  
ПО ДИСЦИПЛИНЕ**  
Практикум по компьютерной безопасности

**Код модуля**  
1156402(1)

**Модуль**  
Практикум по компьютерной безопасности

**Екатеринбург**

Оценочные материалы составлены автором(ами):

№ п/п	Фамилия, имя, отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Бродская Лариса Игоревна	без ученой степени, без ученого звания	Старший преподаватель	департамент математики, механики и компьютерных наук
2	Гейн Андрей Александрович		Инженер	Лаборатория распределенных вычислений, исследований моделей, алгоритмов и программ
3	Пьянзина Елена Сергеевна	кандидат физико-математических наук, без ученого звания	Доцент	Кафедра теоретической и математической физики

**Согласовано:**

Управление образовательных программ

Ю.Д. Маева

**Авторы:**

- Гейн Андрей Александрович, Инженер, Лаборатория распределенных вычислений, исследований моделей, алгоритмов и программ
- Пьянзина Елена Сергеевна, Доцент, Кафедра теоретической и математической физики

**1. СТРУКТУРА И ОБЪЕМ ДИСЦИПЛИНЫ Практикум по компьютерной безопасности**

1.	Объем дисциплины в зачетных единицах	6	
2.	Виды аудиторных занятий	Практические/семинарские занятия	
3.	Промежуточная аттестация	Экзамен	
4.	Текущая аттестация	Домашняя работа	1

**2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ Практикум по компьютерной безопасности**

Индикатор – это признак / сигнал/ маркер, который показывает, на каком уровне обучающийся должен освоить результаты обучения и их предъявление должно подтвердить факт освоения предметного содержания данной дисциплины, указанного в табл. 1.3 РПМ-РПД.

Таблица 1

Код и наименование компетенции	Планируемые результаты обучения (индикаторы)	Контрольно-оценочные средства для оценивания достижения результата обучения по дисциплине
1	2	3
ПК-4 -Способен разрабатывать и реализовывать алгоритмы на базе современных языков программирования и пакетов прикладных программ, осуществлять обоснованный выбор программно-аппаратных средств (Математика и компьютерные науки)	Д-1 - Проявлять умения анализировать и систематизировать информацию З-4 - Сформулировать методы и средства защиты информации П-3 - Осуществлять обоснованный выбор используемых методов защиты информации У-3 - Определять оптимальные методы обеспечения защиты информации	Домашняя работа Практические/семинарские занятия Экзамен
ПК-4 -Готовность к разработке алгоритмов и реализации их на базе	Д-1 - Проявлять умения анализировать и систематизировать информацию	Домашняя работа Практические/семинарские занятия Экзамен

языков программирования и пакетов прикладных программ, осуществлять выбор программно-аппаратных средств (Математическое обеспечение и администрирование информационных систем)	З-4 - Сформулировать методы и средства защиты информации П-3 - Осуществлять обоснованный выбор используемых методов защиты информации У-3 - Определять оптимальные методы обеспечения защиты информации	
--	---	--

### 3. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ МОДУЛЯ В БАЛЬНО-РЕЙТИНГОВОЙ СИСТЕМЕ (ТЕХНОЛОГИЧЕСКАЯ КАРТА БРС)

#### 3.1. Процедуры текущей и промежуточной аттестации по дисциплине

<b>1. Лекции: коэффициент значимости совокупных результатов лекционных занятий – не предусмотрено</b>		
Текущая аттестация на лекциях	Сроки – семестр, учебная неделя	Максимальная оценка в баллах
Весовой коэффициент значимости результатов текущей аттестации по лекциям – <b>не предусмотрено</b>		
Промежуточная аттестация по лекциям – <b>нет</b> Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – <b>не предусмотрено</b>		
<b>2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – 1</b>		
Текущая аттестация на практических/семинарских занятиях	Сроки – семестр, учебная неделя	Максимальная оценка в баллах
<i>домашняя работа</i>	17	50
<i>активность на занятиях</i>	17	50
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям – <b>0.4</b>		
Промежуточная аттестация по практическим/семинарским занятиям – <b>экзамен</b> Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям – <b>0.6</b>		
<b>3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий – не предусмотрено</b>		
Текущая аттестация на лабораторных занятиях	Сроки – семестр, учебная неделя	Максимальная оценка в баллах

<b>Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям -не предусмотрено</b>		
<b>Промежуточная аттестация по лабораторным занятиям –нет</b>		
<b>Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям – не предусмотрено</b>		
<b>4. Онлайн-занятия: коэффициент значимости совокупных результатов онлайн-занятий –не предусмотрено</b>		
<b>Текущая аттестация на онлайн-занятиях</b>	<b>Сроки – семестр, учебная неделя</b>	<b>Максимальная оценка в баллах</b>
<b>Весовой коэффициент значимости результатов текущей аттестации по онлайн-занятиям -не предусмотрено</b>		
<b>Промежуточная аттестация по онлайн-занятиям –нет</b>		
<b>Весовой коэффициент значимости результатов промежуточной аттестации по онлайн-занятиям – не предусмотрено</b>		

### 3.2. Процедуры текущей и промежуточной аттестации курсовой работы/проекта

<b>Текущая аттестация выполнения курсовой работы/проекта</b>	<b>Сроки – семестр, учебная неделя</b>	<b>Максимальная оценка в баллах</b>
<b>Весовой коэффициент текущей аттестации выполнения курсовой работы/проекта– не предусмотрено</b>		
<b>Весовой коэффициент промежуточной аттестации выполнения курсовой работы/проекта– защиты – не предусмотрено</b>		

## 4. КРИТЕРИИ И УРОВНИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ МОДУЛЯ

4.1. В рамках БРС применяются утвержденные на кафедре/институте критерии (признаки) оценивания достижений студентов по дисциплине модуля (табл. 4) в рамках контрольно-оценочных мероприятий на соответствие указанным в табл.1 результатам обучения (индикаторам).

Таблица 4

### Критерии оценивания учебных достижений обучающихся

<b>Результаты обучения</b>	<b>Критерии оценивания учебных достижений, обучающихся на соответствие результатам обучения/индикаторам</b>
Знания	Студент демонстрирует знания и понимание в области изучения на уровне указанных индикаторов и необходимые для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Умения	Студент может применять свои знания и понимание в контекстах, представленных в оценочных заданиях, демонстрирует освоение умений на уровне указанных индикаторов и необходимых для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Опыт /владение	Студент демонстрирует опыт в области изучения на уровне указанных индикаторов.

Другие результаты	<p>Студент демонстрирует ответственность в освоении результатов обучения на уровне запланированных индикаторов.</p> <p>Студент способен выносить суждения, делать оценки и формулировать выводы в области изучения.</p> <p>Студент может сообщать преподавателю и коллегам своего уровня собственное понимание и умения в области изучения.</p>
-------------------	---

4.2 Для оценивания уровня выполнения критериев (уровня достижений обучающихся при проведении контрольно-оценочных мероприятий по дисциплине модуля) используется универсальная шкала (табл. 5).

Таблица 5

### Шкала оценивания достижения результатов обучения (индикаторов) по уровням

Характеристика уровней достижения результатов обучения (индикаторов)				
№ п/п	Содержание уровня выполнения критерия оценивания результатов обучения (выполненное оценочное задание)	Шкала оценивания		
		Традиционная характеристика уровня		Качественная характеристика уровня
1.	Результаты обучения (индикаторы) достигнуты в полном объеме, замечаний нет	Отлично (80-100 баллов)	Зачтено	Высокий (В)
2.	Результаты обучения (индикаторы) в целом достигнуты, имеются замечания, которые не требуют обязательного устранения	Хорошо (60-79 баллов)		Средний (С)
3.	Результаты обучения (индикаторы) достигнуты не в полной мере, есть замечания	Удовлетворительно (40-59 баллов)		Пороговый (П)
4.	Освоение результатов обучения не соответствует индикаторам, имеются существенные ошибки и замечания, требуется доработка	Неудовлетворительно (менее 40 баллов)	Не зачтено	Недостаточный (Н)
5.	Результат обучения не достигнут, задание не выполнено	Недостаточно свидетельств для оценивания		Нет результата

## 5. СОДЕРЖАНИЕ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ПО ДИСЦИПЛИНЕ МОДУЛЯ

5.1. Описание аудиторных контрольно-оценочных мероприятий по дисциплине модуля

### 5.1.1. Практические/семинарские занятия

Примерный перечень тем

1. Структура и форматы исполняемых файлов. 2. Обратный инжиниринг. 3. Бинарные уязвимости. 4. Уязвимость форматной строки. 5. Администрирование образа виртуальной машины. 6. Работа со сниффером трафика. Анализ трафика. 7. Поиск уязвимостей. 8. Системы виртуализации. Системы контейнеризации. 9. Системы изоляции и ограничений. 10. Написание эксплойтов. 11. Использование библиотек для сетевого взаимодействия. 12. Backconnect-шеллы

Примерные задания

Практикум по бинарным уязвимостям. Отладчик. GDB. Переполнение стека. Переполнение кучи. Исполнение кода, шеллкод. Уязвимость форматной строки.

Работы с игровой виртуальной машиной, настройка сети, исследование трафика, работа с незнакомыми операционными системами, сетевыми протоколами и другими технологиями.

Участие в соревнованиях. Разработка собственных заданий для соревнований

LMS-платформа – не предусмотрена

## **5.2. Описание внеаудиторных контрольно-оценочных мероприятий и средств текущего контроля по дисциплине модуля**

Разноуровневое (дифференцированное) обучение.

### **Базовый**

#### **5.2.1. Домашняя работа**

Примерный перечень тем

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 CTF-соревнование 6. Настройте автоматическую работу с пулом виртуальных машин на основе VMWare или Virtual Box. Должно поддерживаться автоматическое 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 rwn 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.

Примерные задания

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 CTF-соревнование

6. Настройте автоматическую работу с пулом виртуальных машин на основе VMWare или Virtual Box. Должно поддерживаться автоматическое 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 rwp

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.

LMS-платформа – не предусмотрена

### 5.3. Описание контрольно-оценочных мероприятий промежуточного контроля по дисциплине модуля

#### 5.3.1. Экзамен

Список примерных вопросов

1. 1. Форматы исполняемых файлов. 2. Формат PE. 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

LMS-платформа – не предусмотрена

### 5.4 Содержание контрольно-оценочных мероприятий по направлениям воспитательной деятельности

Направление воспитательной деятельности	Вид воспитательной деятельности	Технология воспитательной деятельности	Компетенция	Результаты обучения	Контрольно-оценочные мероприятия
Профессиональное воспитание	учебно-исследовательская, научно-исследовательская	Технология формирования уверенности и готовности к самостоятельной успешной профессиональной деятельности	ПК-4	З-4 У-3 П-3	Домашняя работа Практические/семинарские занятия Экзамен