ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

Основы компьютерной безопасности

Код модуля	Модуль
1156492(1)	Основы 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	Пьянзина Елена Сергеевна	кандидат физико-математических наук, без ученого звания	Доцент	Кафедра теоретической и математической физики

Согласовано:

Управление образовательных программ Ю.Д. Маева

Авторы:

- **Бродская Лариса Игоревна, Старший преподаватель, департамент математики, механики и компьютерных наук**
- **Пьянзина Елена Сергеевна, Доцент, Кафедра теоретической и математической физики**

1. СТРУКТУРА И ОБЪЕМ ДИСЦИПЛИНЫ Основы компьютерной безопасности

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

2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ Основы 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 -Готовность к разработке алгоритмов и реализации их на базе языков программирования и пакетов прикладных программ, осуществлять выбор программно-аппаратных средств	Д-1 - Проявлять умения анализировать и систематизировать информацию П-3 - Осуществлять обоснованный выбор используемых методов защиты информации У-3 - Определять оптимальные методы обеспечения защиты информации	Домашняя работа Лекции Практические/семинарские занятия Экзамен
ПК-5 -Способность собирать, обрабатывать и интерпретировать данные современных научных исследований,	З-1 - Сформулировать математически корректную постановку задачи	Домашняя работа Лекции Практические/семинарские занятия Экзамен

необходимые для формирования выводов по соответствующим научным исследованиям		

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

1. Лекции: коэффициент значимости совокупных результатов лекционных занятий – 0.4		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Выполнение тестовых работ по материалам лекций	17	*100*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0.6		
Промежуточная аттестация по лекциям – экзамен **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0.4**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – 0.6		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Работа на практических занятиях	17	60
Выполнение домашних заданий	17	40
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– 1		
Промежуточная аттестация по практическим/семинарским занятиям–нет **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– не предусмотрено**		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий –не предусмотрено		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям -не предусмотрено		
Промежуточная аттестация по лабораторным занятиям –нет **Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям – не предусмотрено**		

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

3.2. Процедуры текущей и промежуточной аттестации курсовой работы/проекта

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

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

Результаты обучения	**Критерии оценивания учебных достижений, обучающихся на соответствие результатам обучения/индикаторам**
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	Студент демонстрирует ответственность в освоении результатов обучения на уровне запланированных индикаторов. Студент способен выносить суждения, делать оценки и формулировать выводы в области изучения. Студент может сообщать преподавателю и коллегам своего уровня собственное понимание и умения в области изучения.

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. Лекции

Самостоятельное изучение теоретического материала по темам/разделам лекций в соответствии с содержанием дисциплины (п. 1.2. РПД)

5.1.2. Практические/семинарские занятия

Примерный перечень тем

1. 1. Симметричное шифрование. 2. Асимметричное шифрование. 3. Хеш-функции. 4. Стегоанализ. 5. Протокол TCP/IP. 6. Протокол DNS. 7. Протоколы FTP, SNTP. Сети VPN.

8. Протоколы HTTP, HTTPS, SSL, TLS. 9. SQL- и noSQL-инъекции. 10.Операционные системы. GNU и FSF. Стандарт POSIX. 11. Дистрибутивы Linux. Загрузка системы. Ядро Linux. 12. Пользователи в Linux. Командная строка. 13. Виртуальные машины Linux. 14. Ассемблер. 15. Структура и форматы исполняемых файлов. 16. Обратный инжиниринг. 17. Бинарные уязвимости. 18. Уязвимость форматной строки

Примерные задания

1. Начинающий специалист по информационной безопасности Боб переслал Алисе сообщение, зашифрованное шифрами из OpenSSL, но забыл порядок их применения. Даны шифры и ключи, помогите Алисе расшифровать сообщение!

2. Восстановите пароль от Windows, если LM-хеш от него равен BE1DF386397C0288AAD3B435B51404EE

3. Восстановите информацию, стеганографированную с помощью LSB.

4. Восстановите пароль от Oracle database по дампу трафика проведённой атаки

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. 1) Криптография 2) Хеши 3) Стеганография 4) Компьютерные сети 5) Протоколы прикладного уровня 6) SQL-инъекции и инъекции в команды ОС 7) Linux, работа с виртуальными машинами 8) Работа с удаленным сервером по SSH, bash 9) Обратный инжиниринг 10) Переполнение стека 11) Уязвимость форматной строки

Примерные задания

1. Выполните трансфер DNS-зоны

2. Восстановите словарный пароль для HTTP-аутенфикации по дампу трафика.

3. Выполните SQL-инъекцию

4. Найдите уязвимость в сервисе и проэксплуатируйте её: http://downloader.training.hackerdom.ru/

5. Прочитайте файл на сервере, имея доступ по SSH к «слепому bash» — вы можете отправлять команды, но не видите результат их выполнения.

6. Узнайте верный пароль для прохождения проверок в скомпилированной программе.

7. Узнайте алгоритм работы программы по jar-файлу.

LMS-платформа − не предусмотрена

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

5.3.1. Экзамен

Список примерных вопросов

1. 1. История криптографии. 2. Криптография. Понятие шифрования. 3. Криптография. Симметричное и ассиметричное шифрование. 4. Криптография. Открытый и закрытый ключи. 5. Криптография. Алгоритм Диффи-Хеллмана. 6. Криптография. Алгоритм RSA с доказательством корректности. 7. Криптография. Электронно-цифровая подпись. 8. Криптография. Хеш-функция. 9. Криптография. Криптографическая хеш-функция. 10. Криптография. Хеш-функция MD5. 11. Криптография. Коллизии первого и второго рода. 12. Криптография. Архитектура и экономика криптовалюты Bitcoin. 13. История стеганографии. 14. Стеганография. Компьютерная стеганография. 15. Стеганография. Текстовая стеганография. 16. Стеганография. Стеганография в изображениях, звуковом и видеофайле. 17. Стеганография. Стеганография в форматах с потерями (на примере JPEG). 18. Стеганография. Стегоанализ. 19. Стеганография. Цифровые водяные знаки. 20. Сети. Стек протоколов ISO/OSI. 21. Сети. Стек протоколов TCP IP. 22. Сети. Физический уровень. 23. Сети. Канальный уровень: протокол Ethernet. 24. Сети. Протокол DHCP. 25. Сети. Протокол ARP. 26. Сети. Сетевой уровень: протокол IP. 27. Сети. IP-маршрутизация. 28. Сети. IPv4 и IPv6. 29. Сети. Протоколы прикладного уровня. 30. Сети. Протокол DNS. 31. Сети. Иерархия NS-серверов. 32. Сети. Отравление кеша DNS. 33. Сети. Протокол FTP. 34. Сети. Протокол SMTP. 35. Сети. Туннелирование. 36. Сети. Построение частных сетей VPN. 37. История протокола HTTP. 38. Структура HTTP-запроса и ответа.URL. 39. Методы HTTP. 40. Заголовки HTTP. 41. Авторизация и аутенфикация посредством HTTP. 42. Протоколы HTTPS, SSL и TLS. 43. Инъекции. 44. Инъекции. 45. SQL-инъекции. 46. Синтаксис SQL. 47. UNION. 48. Экранирование символов при инъекции. 49. Множественные запросы. 50. Слепые SQL-инъекции. 51. NoSQL-инъекции. 52. LDAP-инъекции. 53. XPath-инъекции. 54. Инъекции в командах операционных систем. 55. GNU и FSF. 56. Стандарт POSIX. 57. История ядра Linux. 58. Дистрибутивы Linux. 59. Unix Way. 60. Загрузка системы. 61. GRUB. 62. Пользователи в Linux. 63. Командная строка. 64. Виртуальные машины. 65. Сброс пароля. 66. Архитектура компьютера. 67. Принципы фон Неймана. 68. Регистры процессора. 69. Ассемблер. 70. Команда MOV. 71. Арифметические и логические команды. 72. Знаковые и беззнаковые числа. 73. Условный и безусловные переходы. 74. Управление выполнение программы. 75. Функции. 76. Структура исполняемого файла. 77. Форматы исполняемых файлов. 78. Формат PE. 79. Шаблоны исполняемого кода. 80. Шаблоны объектно-ориентированного программирования. 81. Пакеты. 82. Антиотладка. 83. Отладчик. 84. GDB. 85. Переполнение стека. 86. Переполнение кучи. 87. Исполнение кода, шеллкод. 88. OpenSSL Heartbleed. 89. Уязвимость форматной строки.

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-исследовательск	Технология формирования уверенности и готовности к	ПК-4	У-3 П-3 Д-1	Домашняя работа Лекции Практические/семинарские занятия

	ая	самостоятельной успешной профессиональной деятельности			Экзамен