ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ПО ДИСЦИПЛИНЕ
Практические аспекты информационной безопасности

Код модуля	Модуль
1156404(1)	Практические аспекты информационной безопасности

Екатеринбург

Оценочные материалы составлены автором(ами):

№ п/п	Фамилия, имя, отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Баранский Виталий Анатольевич	доктор физико-математических наук, профессор	Профессор	алгебры и фундаментальной информатики
2	Бродская Лариса Игоревна	без ученой степени, без ученого звания	Старший преподаватель	департамент математики, механики и компьютерных наук
3	Копейцев Вячеслав Ефимович	без ученой степени, без ученого звания	Старший преподаватель	департамент математики, механики и компьютерных наук

Согласовано:

Управление образовательных программ Ю.Д. Маева

Авторы:

- **Баранский Виталий Анатольевич, Профессор, алгебры и фундаментальной информатики**
- **Бродская Лариса Игоревна, Старший преподаватель, департамент математики, механики и компьютерных наук**
- **Копейцев Вячеслав Ефимович, Старший преподаватель, департамент математики, механики и компьютерных наук**

1. СТРУКТУРА И ОБЪЕМ ДИСЦИПЛИНЫ Практические аспекты информационной безопасности

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

2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ Практические аспекты информационной 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-2 -Способен математически корректно ставить естественнонаучные задачи, обрабатывать научную информацию и результаты исследований, определять закономерности предметной области (Математика и компьютерные науки)	Д-2 - Демонстрировать умения анализировать и обобщать информацию, делать логические умозаключения П-3 - Иметь практический опыт проведения экспериментов и наблюдений, обобщения и обработки информации	Домашняя работа № 1 Домашняя работа № 2 Практические/семинарские занятия Экзамен
ПК-4 -Способен разрабатывать и реализовывать	З-4 - Сформулировать методы и средства защиты информации	Домашняя работа № 1 Домашняя работа № 2

алгоритмы на базе современных языков программирования и пакетов прикладных программ, осуществлять обоснованный выбор программно-аппаратных средств (Математика и компьютерные науки)	У-3 - Определять оптимальные методы обеспечения защиты информации	Практические/семинарские занятия Экзамен
ПК-4 -Готовность к разработке алгоритмов и реализации их на базе 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 У-3 - Определять оптимальные методы обеспечения защиты информации	Домашняя работа № 1 Домашняя работа № 2 Практические/семинарские занятия Экзамен
ПК-5 -Способность собирать, обрабатывать и интерпретировать данные современных научных исследований, необходимые для формирования выводов по соответствующим научным исследованиям (Математическое обеспечение и администрирование информационных систем)	Д-2 - Демонстрировать умения анализировать и обобщать информацию, делать логические умозаключения П-3 - Иметь практический опыт проведения экспериментов и наблюдений, обобщения и обработки информации	Домашняя работа № 1 Домашняя работа № 2 Практические/семинарские занятия Экзамен

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 – не предусмотрено		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по лекциям – не предусмотрено		
Промежуточная аттестация по лекциям – нет **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – не предусмотрено**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – 1		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
домашняя работа №1	6,8	50
домашняя работа №2	6,15	50
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– 0.5		
Промежуточная аттестация по практическим/семинарским занятиям–экзамен **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– 0.5**		
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)		
№	**Содержание уровня**	**Шкала оценивания**

п/п	выполнения критерия оценивания результатов обучения (выполненное оценочное задание)	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. Основы сетевых технологий
2. Проблемы информационной безопасности в сетевых технологиях 1.
3. Проблемы информационной безопасности в сетевых технологиях 2.
4. Протоколы прикладного уровня.
5. Безопасность веб-сервера.
6. Методы скрытого хранения информации.
7. Работа исполняемых файлов в современных операционных системах.
8. Методы статического анализа исполняемых файлов.
9. Методы динамического анализа исполняемых файлов.
10. Различные проблемы безопасности исполняемых файлов.
11. Методы противодействия проникновению в систему.
12. Принципы работы современного антивирусного ПО.

Примерные задания

Принципы работы с утилитой Wireshark. Разбор методов анализа входящего и исходящего се-тевого трафика, методов поиска и фильтрации сетевых пакетов. Анализ содержимого не-скольких произвольных пакетов различных протоколов, для подтверждения теоретических основ. Анализ практического примера скрытой передачи данных с использованием протокола

ICMP.

Изучение методов противодействия перехвату сетевого трафика в Wi-Fi сетях. Обнаружение существования прокси-сервера между компьютером и сервером назначения. Изменение па-раметров прокси сервера с использованием средств, предоставляемых операционной систе-мой. Применение различных средств перенаправления трафика, онлайн решений, VPN под-ключений. Моделирование ситуации перехвата аутентификационных данных, при работе с веб-ресурсом, а также перехвата файлов cookie. Подмена прокси-сервера с использованием PAC файлов, как пример типичных действий вредоносного программного обеспечения, мето-ды противодействия этому.

Изучение практических аспектов работы сервиса DNS, наглядный разбор действий, применя-емых вредоносным ПО на локальной системе для подмены IP адресов веб-ресурсов. В частно-сти, техники, применяемые для сокрытия текста в файле hosts операционной системы Win-dows. Воспроизведение перехвата запроса и подмены ответа на DNS запрос (техника dns spoofing) и применение методов противодействия этому. В частности, случайное изменение номера DNS запроса. Решение задачи поиска поддоменов произвольного домена по средствам применения сервиса DNS.

Рассмотрение примеров веб-ресурсов с различными типами используемых сертификатов, их преимуществ и недостатков. Создание собственных сертификатов в операционных системах Windows и Unix, установка созданных сертификатов в указанных операционных системах. Проверка работы защищённого подключения с использованием созданных сертификатов. Практическое рассмотрение техник подмены сертификата на промежуточном узле связи (техника man-in-the-middle) и методов защиты от них.

Применение утилит сканирования портов удалённого сервера с изучением методов идентификации программного обеспечения, работающего на сервере. Анализ сетевого трафика от клиента, до специально подготовленного веб-сервера. Обсуждение со студентами проблем рассматриваемого протокола сетевого обмена. Применение техник аудита безопасности работы сервера с базой данных. Базовые техники SQL Injection. Применение техник аудита безопасности работы сервера с данными, участвующими в динамическом создании страниц. Базовые техники XSS. Применение на специально подготовленном сервере методов защиты от атак типа отказ в обслуживании.

Внесение изменений в произвольный файл (изображение) с целью скрытого хранения информации без изменения и порчи его основного содержимого. Решение специально подготовленных заданий, направленных на поиск и извлечение скрытых данных. В число таких задач входит анализ: изображения, аудиофайла, образа (полной копии) содержимого сменного носителя информации.

Рассмотрение основного и дополнительного заголовков файла, а также описание назначения различных полей, интересующих исследователя в контексте информационной безопасности. Рассмотрение различных таблиц и секций исполняемого файла. Анализ изменений, происхо-дящих с загруженным в память исполняемым файлом в результате создания процесса опера-ционной системой. Рассмотрение различных типов сборки и компоновки исполняемых фай-лов.

Студентам предлагается для решения множество заранее подготовленных заданий, являющихся исполняемыми файлами PE-EXE, работающими под управлением операционной системы Windows, а также ELF, работающими под управлением операционной системы Ubuntu. Цель данного раздела – изучение практических аспектов использования интерактивного дизассемблера IDA. Также, рассматривается различный дополнительный инструментарий ди-

зассемблера, например, создание структур, исполнение кода, техники ручного и автоматического распознавания функций.

Тема является логическим продолжением предыдущего раздела, на нём студенты используют специально подготовленные исполняемые файлы, статический анализ которых специально затруднён. Сначала используется локальный отладчик интерактивного дизассемблера IDA, затем удалённый отладчик того же приложения, после чего студенты переходят к работе с отладчиком OllyDbg.

Последней задачей является отладка уже ранее запущенного процесса с применением методов сокрытия работы отладчика в системе.

Как и в предыдущих разделах, студентам предлагается набор специально подготовленных за-даний, состоящий из исполняемых файлов, однако на этот раз они содержат бинарные уязви-мости. Студенты должны на основе материалов лекций и указаний преподавателя обнару-жить уязвимости, создать программный код, который в учебных целях будет применён на данных файлах и получит управление. После этого производится анализ выявленных проблем безопасности с применением различных вариантов решения задачи устранения уязвимостей в исполняемых файлах.

Практическое рассмотрение техник настройки программного обеспечения и операционной системы для затруднения проведения атак на систему. Настройка различного программного обеспечения и операционной системы для ведения записи всех необходимых событий – ло-гов, что является неотъемлемой частью аудита информационной безопасности. Настройка фильтрации пакетов на корпоративном прокси-сервере, а также настройка различных спам-фильтров и сетевых экранов. Методы сбора информации на скомпрометированной системе, в частности анализ логов, памяти, изменений в файловой системе и т.д.

Рассмотрение различных образцов программного обеспечения, специально подготовленных в учебных целях и имитирующих работу вредоносного программного обеспечения. Задача дан-ного раздела заключается в анализе данных программ и написании алгоритмов отката изме-нений в системе, полученных в следствии запуска данных приложений, что имитирует задачу написания алгоритма устранения последствий работы вредоносного программного обеспече-ния.

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 № 1

Примерный перечень тем

1. Проблемы информационной безопасности в сетевых технологиях 2.

Примерные задания

Студенту выдается запись сетевого трафика в формате pcapng с машины, предположительно зараженной вредоносным ПО. Целью ставится выявление следов сетевой активности деструк-тивных программ, а также анализ переданных данных.

В частности, требуется определить какие данные были переданы с зараженной машины, а так-же по какому IP адресу располагается сервер управления вредоносным ПО и какому доменно-му имени происходило обращение к нему. Для поиска необходимых данных требуется исполь-зовать интерфейс приложения Wireshark и правила фильтрации сетевых пакетов, изученные в курсе.

Требуется дать описание атаки типа DNS Cache poisoning на систему DNS. Ответом на задачу является описание уязвимостей архитектуры и протокола системы, приводящим к данной уяз-вимости. Также, требуется описать ошибки в конфигурации DNS серверов, приводящие к воз-можности эксплуатации уязвимости. Кроме этого, необходимо указать методы защиты от атак данного типа.

LMS-платформа − не предусмотрена

5.2.2. Домашняя работа № 2

Примерный перечень тем

1. Безопасность веб-сервера.

Примерные задания

Студенту выдается фрагмент кода веб-страницы.

Требуется определить, содержит ли данный код уязвимости, если да, уязвимости какого типа имеются. Также, при наличии уязвимостей требуется описать вектор атаки, последствия, к ко-торым может привести эксплуатация имеющихся уязвимостей, а также дать рекомендации по мерам защиты от описываемых атак.

LMS-платформа − не предусмотрена

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

5.3.1. Экзамен

Список примерных вопросов

1. 1. Разбор методов анализа входящего и исходящего сетевого трафика, методов поиска и фильтрации сетевых пакетов.
2. 2. Поиск следов скрытой передачи данных в сетевом трафике.
3. 3. Методы противодействия перехвату сетевого трафика в Wi-Fi сетях.
4. 4. Обнаружение существования прокси-сервера между компьютером и сервером назначе-ния сетевых данных.
5. 5. Типовые методы перехвата и подмены сетевого трафика.
6. 6. Угрозы, связанные с использованием DNS и пути их решения.
7. 7. Техники подмены сертификата на промежуточном узле связи (техника man-in-the-middle) и методов защиты от них.
8. 8. Методы идентификации программного обеспечения.
9. 9. Потенциальные уязвимости серверов баз данных.
10. 10. Базовые техники SQL Injection и защита от них.
11. 11. Базовые техники XSS и защита от них.

12. 12. Применение на серверной системе методов защиты от атак типа отказ в обслуживании.

13. 13. Методы сокрытия информации внутри графических файлов и техники обнаружения по-добных фактов.

14. 14. Техники проведения аудита безопасности серверных систем.

15. 15. Техники проведения аудита безопасности рабочих станций.

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	Домашняя работа № 1 Домашняя работа № 2 Практические/семинарские занятия Экзамен