ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ПО ДИСЦИПЛИНЕ

Экспертная и аналитическая деятельность в сфере обеспечения безопасности объектов КИИ

Код модуля	Модуль
1156044(1)	Обнаружение и предупреждение компьютерных атак на объектах критической информационной инфраструктуры (КИИ)

Екатеринбург

Оценочные материалы составлены автором(ами):

№ п/п	Фамилия, имя, отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Коллеров Андрей Сергеевич	к.т.н., доцент	доцент	УНЦ ИБ
2	Пономарева Ольга Алексеевна	-, -	старший преподаватель	УНЦ ИБ

Согласовано:

Управление образовательных программ Т.Г. Комарова

Авторы:

- **Коллеров Андрей Сергеевич, доцент, УНЦ ИБ**
- **Пономарева Ольга Алексеевна, старший преподаватель, УНЦ ИБ**

1. СТРУКТУРА И ОБЪЕМ ДИСЦИПЛИНЫ Экспертная и аналитическая деятельность в сфере обеспечения безопасности объектов КИИ

1.	**Объем дисциплины в зачетных единицах**	4	
2.	**Виды аудиторных занятий**	Лекции Лабораторные занятия	
3.	**Промежуточная аттестация**	Экзамен	
4.	**Текущая аттестация**	Контрольная работа	1
		Домашняя работа	1

2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ Экспертная и аналитическая деятельность в сфере обеспечения безопасности объектов КИИ

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-5 -Способен разработать и смоделировать программно-технические средства защиты информации от несанкционированного доступа	З-10 - Различать средства проектирования электронных схем З-8 - Использовать средства контроля защищенности информации от несанкционированного доступа З-9 - Различать методики контроля защищенности информации от несанкционированного доступа П-1 - Разрабатывать технический (эскизный) проект программно-технического средства защиты информации от несанкционированного	Домашняя работа Контрольная работа Лабораторные занятия Лекции Экзамен

	доступа и специальных воздействий на нее П-3 - Разрабатывать рабочую и эксплуатационную документацию на техническое средство защиты У-1 - Разрабатывать техническое задание на создание программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее У-3 - Разрабатывать программы и методики испытаний программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее	

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 – 0.50		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
контрольная работа	*3,5*	*100*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0.50		
Промежуточная аттестация по лекциям – экзамен **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0.50**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – не предусмотрено		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– не предусмотрено		
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 –0.50		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
домашняя работа	3,15	100
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям -1.00		
Промежуточная аттестация по лабораторным занятиям –нет **Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям – 0.00**		
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. Лабораторные занятия

Примерный перечень тем

1. Обнаружение компьютерных атак на узлы сети с использованием комплекса Cisco IDS Sensor
2. Обнаружение компьютерных атак на узлы сети с использованием комплекса Cisco MARS
3. Обнаружение компьютерных атак на узлы сети с использованием СОА Cisco Security Agent и Cisco MARS
4. Установка и настройка Malcom
5. Захват и анализ трафика с помощью Malcom
6. Извлечение данных при помощи команды SELECT языка SQL
7. Ограничение и сортировка данных
8. Однострочные функции
9. Функции преобразования данных. Общие функции. Условные выражения
10. Агрегирование данных с использованием групповых функций
11. Выборка данных. Работа с несколькими таблицами
12. Использование операторов работы над множествами
13. Манипулирование большими данными
14. Работа с различными временными зонами
15. Выборка данных с использованием подзапросов
16. Работа с иерархическими данными

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. Контрольная работа

Примерный перечень тем

1. Аналитическая работа с СОА при помощи СУБД
2. Обработка массивов трафика
3. Выборка данных из СУБД

Примерные задания

1. Дополните утверждение

Согласно федеральному законодательству состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак — это …

а) безопасность критической информационной инфраструктуры;

б) защита информации критической информационной инфраструктуры;

в) система защиты критической информационной инфраструктуры;

г) надежность критической информационной инфраструктуры.

2. Дополните утверждение

Согласно федеральному законодательству Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации представляет собой …

а) единый территориально распределенный комплекс, включающий силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;

б) комплекс программных и программно-аппаратных средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;

в) совокупность объектов критической информационной инфраструк-туры, которым присвоена одна из категорий значимости и которые включены в реестр значимых объектов критической информационной инфраструктуры;

г) информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности.

3. Отметьте правильный ответ

Совокупность специальным образом организованных данных, хранимых в памяти вычислительной системы и отображающих состояние объектов и их взаимосвязей в рассматриваемой предметной области - это

а) База данных;

б) СУБД;

в) Словарь данных;

г) Информационная система;

д) Вычислительная система.

LMS-платформа − не предусмотрена

5.2.2. Домашняя работа

Примерный перечень тем

1. Провести анализ защищенности объекта КИИ

Примерные задания

1. Развернуть виртуальную настройку компьютерной сети для объекта КИИ

2. Создайте и продемонстрируйте работоспособность сигнатуры обнаружения атаки XSS

3. Произвести настройку сетевых интерфейсов

4. Создать отчет, в котором отражается иерархия управления защищаемого объекта, начиная с сотрудника по фамилии Кинг. Вывести фамилии, номера менеджеров и номера телефонов. Назвать столбцы, как показано в примере выходных результатов

5. Написать запрос для нахождения всех атак, оценка уязвимости которых больше среднего значения CVSS по организации (жертве), на которую была направлена атака. Вывести эксплуатируемую уязвимость, её оценку, идентификатор жертвы и среднее значение CVSS по организации (жертве). Отсортировать результаты по последнему столбцу и округлить его до двух знаков после запятой

6.Оформить отчет по домашней работе

LMS-платформа − не предусмотрена

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

5.3.1. Экзамен

Список примерных вопросов

1. Организация центра мониторинга информационной безопасности
2. Реестр уязвимостей БДУ ФСТЭК России
3. Нормативное регулирование деятельности центров ГосСОПКА
4. Функции центра мониторинга информационной безопасности
5. Архитектура центра мониторинга информационной безопасности
6. Стандарт Common Vulnerabilities and Exposures
7. Агрегаторы информации об уязвимостях
8. Подключение и взаимодействие с НКЦКИ
9. Реагирование на компьютерный инцидент
10. Архитектура и функционал Malcolm
11. Извлечение данных при помощи команды SELECT языка SQL
12. Ограничения и сортировка данных в СУБД Oracle
13. Однострочные функции в СУБД Oracle
14. Функции преобразования данных в СУБД Oracle

LMS-платформа − не предусмотрена

5.4 Содержание контрольно-оценочных мероприятий по направлениям воспитательной деятельности

Направления воспитательной деятельности сопрягаются со всеми результатами обучения компетенций по образовательной программе, их освоение обеспечивается содержанием всех дисциплин модулей.