ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ПО ДИСЦИПЛИНЕ

Экспертно-аналитическая деятельность в центрах мониторинга ГосСОПКА

Код модуля	**Модуль**
1156043(1)	Организация и функционирование центров мониторинга Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА)

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
3	Фартушный Андрей Владимирович	без ученой степени, без ученого звания	Ассистент	

Согласовано:

Управление образовательных программ Т.Г. Комарова

Авторы:

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

1. СТРУКТУРА И ОБЪЕМ ДИСЦИПЛИНЫ Экспертно-аналитическая деятельность в центрах мониторинга ГосСОПКА

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 Экспертно-аналитическая деятельность в центрах мониторинга ГосСОПКА

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 – 0.5		
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 – 0.5		
Промежуточная аттестация по лекциям – экзамен **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0.5**		
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 –0.5		
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		
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. Лабораторные занятия

Примерный перечень тем

1. Установка и настройка Malcom
2. Захват и анализ трафика с помощью Malcom
3. Извлечение данных при помощи команды SELECT языка SQL
4. Ограничение и сортировка данных
5. Функции преобразования данных. Общие функции. Условные выражения
6. Агрегирование данных с использованием групповых функций
7. Выборка данных. Работа с несколькими таблицами

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.
4. Проектирование сегмента сети для отработки навыков проведения аудита информационной безопасности.

Примерные задания

1. Отметьте правильный ответ

Информационная система - это

а) Любая система обработки информации;

б) Система обработки текстовой информации;

в) Система обработки графической информации;

г) Система обработки табличных данных;

д) Нет верного варианта.

Отметьте правильный ответ

Разновидность информационной системы, в которой реализованы функции централизованного хранения и накопления обработанной информации организованной в одну или несколько баз данных это

а) Банк данных;

б) База данных;

в) Информационная система;

г) Словарь данных;

д) Вычислительная система.

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.

Отметьте правильный ответ

Комплекс языковых и программных средств, предназначенный для создания, ведения и совместного использования БД многими пользователями - это

а) СУБД;

б) База данных;

в) Словарь данных ;

г) Вычислительная система;

д) Информационная система.

Отметьте правильный ответ

Подсистема банка данных, предназначенная для централизованного хранения информации о структурах данных, взаимосвязях файлов БД друг с другом, типах данных и форматах их представления, принадлежности данных пользователям, кодах защиты и разграничения доступа и т.п. — это

а) Словарь данных;

б) Информационная система;

в) Вычислительная система;

г) СУБД;

д) База данных.

LMS-платформа − не предусмотрена

5.2.2. Домашняя работа

Примерный перечень тем

1. Разработка запросов экспертно-аналитической деятельности

Примерные задания

1. 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.

2. Создать запрос для вывода эксплуатируемой уязвимости и количество часов с даты обнаружения атаки. Если атака зафиксирована 2 или более часов назад, вывести «более 2 часа назад», если 4 или более часов назад, вывести «более 4 часа назад», если 6 или более часов назад, вывести «более 6 часов назад». При невыполнении ни одного из этих условий вывести «Внимание!». Отсортировать данные по столбцу DETECTION_TIME. Использовать таблицу ATTACKS. Для выполнения задачи устанавливается текущее время равное «22.04.2020 22:06:22» .

3. Написать матричный запрос для вывода всех идентификаторов сетей и количества зафиксированных атак, направленных на эту сеть в организациях с идентификаторами 20, 50, 80 и 90. Последний столбец должен содержать общее количество атак в каждой конкретной сети. Дать столбцам соответствующие заголовки.

4. Написать запрос для вывода следующих данных об атаках, идентификатор администратора которых меньше 120: идентификатор администратора, идентификатор сети, общее количество атак для каждого идентификатора сети, которые подчиняются одному администратору, общее количество атак, сгруппированных по их администраторам, сводные значения по общему количеству атак для каждого идентификатора сети независимо от администратора. Отметить выходные данные, полученные в запросе. Используя функцию GROUPING. Написать запрос для выяснения, являются ли неопределенные значения в столбцах, которые соответствуют приведенным в предложении GROUP BY, результатом применения операции CUBE.

5. 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. Регламентирование в российской нормативной базе деятельности по анализу угроз
4. Функции центра мониторинга информационной безопасности
5. Архитектура центра мониторинга информационной безопасности
6. Стандарт Common Vulnerabilities and Exposures
7. Агрегаторы информации об уязвимостях
8. Сценарии Cyber Kill Chain
9. Применение ATT&CK для моделирования угроз
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
15. Формирование отчетных таблиц 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.