Приложение
к рабочей программе модуля (дисциплины)

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

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

Екатеринбург, 2021

Оценочные материалы по модулю составлены авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Коллеров Андрей Сергеевич	К.т.н., доцент	доцент	*Учебно-научный центр «Информационная безопасность»*

Согласовано:

Управление образовательных программ Р.Х.Токарева

1. СТРУКТУРА И ОБЪЕМ МОДУЛЯ

Организация и функционирование центров мониторинга Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА)

№ п/п	Перечень дисциплин модуля в последовательности их освоения	Объем дисциплин модуля и всего модуля в зачетных единицах и часах	Форма итоговой промежуточной аттестации по дисциплинам модуля и в целом по модулю
1.	Реагирование на компьютерные инциденты, ликвидация их последствий на объектах КИИ	*3/108*	*З*
2	Экспертная и аналитическая деятельность в сфере обеспечения безопасности объектов КИИ	*3/108*	Э
3	Эксплуатация систем обнаружения компьютерных атак на объектах КИИ	*3/108*	Э
	ИТОГО по модулю:	***9/324***	

2. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО МОДУЛЮ

2.1. Проект по модулю

Не предусмотрено

2.2. Интегрированный экзамен по модулю

Не предусмотрено

Раздел 3. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ 1

Модуль *Обнаружение и предупреждение компьютерных атак на объектах критической информационной инфраструктуры (КИИ)*

Дисциплина Реагирование на компьютерные инциденты, ликвидация их последствий на объектах КИИ

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	*Учебно-научный центр «Информационная безопасность»*

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ *Обнаружение и предупреждение компьютерных атак на объектах критической информационной инфраструктуры (КИИ)*

Таблица 1

Код и наименование компетенций, формируемые с участием дисциплины	**Планируемые результаты обучения (индикаторы)**
ПК 3. Способен проводить экспертизу при расследовании компьютерных преступлений, правонарушений и инцидентов.	З-1 Принципы построения компьютерных систем и сетей З-2 Уязвимости компьютерных систем и сетей З-3 Криптографические методы защиты информации З-4 Принципы построения систем управления базами данных З-5 Средства анализа конфигураций З-6 Национальные, межгосударственные и международные стандарты в области защиты информации З-7 Нормативные правовые акты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации З-9 Организационные меры по защите информации У-1 Анализировать компьютерную систему с целью определения уровня защищенности и доверия У-2 Прогнозировать возможные пути развития действий нарушителя информационной безопасности У-3 Производить анализ политики безопасности на предмет адекватности У-4 Проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах У-5 Составлять и оформлять аналитический отчет по результатам проведенного анализа У-6 Разрабатывать предложения по устранению выявленных уязвимостей П-1 Определение уровня защищенности и доверия в компьютерных системах П-2 Оценка рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем П-3 Оценка соответствия механизмов безопасности компьютерной системы требованиям существующих нормативных документов, а также их адекватности существующим рискам

	П-4 Подготовка аналитического отчета по результатам проведенного анализа П-5 Формулирование предложений по устранению выявленных уязвимостей

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ

Анализ событий безопасности и обеспечение функционирования технических средств сегмента ГосСОПКА

2. ВИДЫ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ, ВКЛЮЧАЯ МЕРОПРИЯТИЯ ТЕКУЩЕЙ АТТЕСТАЦИИ

2.1. Распределение объема времени по видам учебной работы

Таблица 2

№ п/п	Наименование дисциплины модуля	Объем времени, отведенный на освоение дисциплины модуля								
		Аудиторные занятия, час.				Промежуточная аттестация (форма итогового контроля /час.)	Контактная работа (час.)	Самостоятельная работа студента, включая текущую аттестацию (час.)	Всего по дисциплине	
		Занятия лекционного типа	Практические занятия	Лабораторные работы	Всего				Час.	Зач. ед.
1	2	3	4	5	6	7	8	9	10	11
1.	*Реагирование на компьютерные инциденты, ликвидация их последствий на объектах КИИ*	36	-	18	54	Э	62,35	43,57	108	3
Всего на освоение дисциплины модуля (час.)		36		18	54	Э	62,35	43,57	108	3

2.2. Виды СРС, количество и объем времени на контрольно-оценочные мероприятия СРС по дисциплине

Контрольно-оценочные мероприятия СРС включают самостоятельное изучение материала, подготовку к аудиторным занятиям и мероприятиям текущего контроля, выполнение и оформление внеаудиторных мероприятий текущего контроля и подготовку к мероприятиям промежуточного контроля.

Таблица 3

№ п/п	Вид самостоятельной работы студента по дисциплине модуля	Количество контрольно-оценочных мероприятий СРС	Объем контрольно-оценочных мероприятий СРС (час.)
1.	*Подготовка к лекционным*	*6*	*10 час.*
2	*Подготовка к практическим занятиям*	*16*	*16 час.*
3.	*Самостоятельное изучение материала*		*8,57*
	Подготовка к экзамену	1	9 час.
	Итого на СРС по дисциплине:		*43,57 час.*

3. КРИТЕРИИ И УРОВНИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ МОДУЛЯ

3.1 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.
Личностные качества	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.

3.2 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

4. СОДЕРЖАНИЕ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ПРОМЕЖУТОЧНОГО КОНТРОЛЯ ДИСЦИПЛИНЕ МОДУЛЯ

Зачет в форме итогового тестирования с использованием ОК при реализации модели исключительно электронного обучения с использованием внутреннего онлайн-курса (ОК) УрФУ http://courses.openedu.urfu.ru/courses/course-v1:UrFU+AOVZ+spring_2018/info

Спецификация теста в системе ОК УрФУ:

Для проведения промежуточной аттестации используется ОК УрФУ.

Структура тестовых материалов при использовании ОК УрФУ: Тест включает в себя 40 заданий, время выполнения – 60 минут. В структуре теста представлены вопросы по всем разделам изучения дисциплины.

Теоретические вопросы

1. Этапы сетевой атаки.
2. Понятие и систематика компьютерных атак.
3. Атаки типа «отказ в обслуживании».
4. Выявление уязвимых мест атакуемой системы.
5. Сигнатурный анализ и обнаружение аномалий.
6. Обнаружение в реальном времени и отложенный анализ.
7. Локальные и сетевые системы обнаружения атак.
8. Распределенные системы обнаружения атак.

9. Понятие многоагентной СОА и ее использование для обнаружения комплексных атак.

10. Алгоритмы и модели СОА. Методы опорных векторов SVM.

11. Алгоритмы и модели СОА. Кластерный анализ.

12. Алгоритмы и модели СОА. Использование аппарата нечеткой логики для обнаружения атак.

13. Параметры сетевого трафика, анализируемые СОА.

14. Ответственность за неправомерное воздействие на КИИ РФ.

15. Основные положения о ГосСОПКА.

Практические вопросы

1. Произвести установку и настройку СОА Snort.
2. Произвести установку и настройку СОА Suricata.
3. Произвести нагрузочное тестирование web-сервера.
4. Создать правило СОА Snort для обнаружения эксплуатации уязвимости типа «Подделка HTTP-запросов».
5. Создать правило СОА Snort для обнаружения эксплуатации уязвимости типа «Внедрение команд».
6. Создать правило СОА Snort для обнаружения эксплуатации уязвимости типа «Обход директории».
7. Создать правило СОА Snort для обнаружения эксплуатации уязвимости типа «Выполнение команд на сервере».
8. Создать правило СОА Snort для обнаружения эксплуатации уязвимости типа «Внедрение операторов SQL».
9. Создать правило СОА Snort для обнаружения эксплуатации уязвимости АСУТП.
10. Подготовить отчет на основе сработавших правил, при использовании резервной копии правил rules1 и дампа сетевого трафика vulnerability1.
11. Подготовить отчет на основе сработавших правил, при использовании резервной копии правил rules2 и дампа сетевого трафика vulnerability2.
12. Подготовить отчет на основе сработавших правил, при использовании резервной копии правил rules3 и дампа сетевого трафика vulnerability3.
13. Подготовить отчет на основе сработавших правил, при использовании резервной копии правил rules4 и дампа сетевого трафика vulnerability4.
14. Подготовить отчет на основе сработавших правил, при использовании резервной копии правил rules5 и дампа сетевого трафика vulnerability5.
15. Получение информации об уязвимостях CVE-2018-0798, CVE-2019-19781, CVE-2020-0601, CVE-2019-10149 и CVE-2019-3396 из баз данных уязвимостей компьютерных систем

Раздел 3. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ 2

Экспертная и аналитическая деятельность в сфере обеспечения безопасности объектов КИИ

Модуль *Обнаружение и предупреждение компьютерных атак на объектах критической информационной инфраструктуры (КИИ)*

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Синадский Николай Игоревич	К.т.н., доцент	доцент	*Учебно-научный центр «Информационная безопасность»*

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ

Обнаружение и предупреждение компьютерных атак на объектах критической информационной инфраструктуры (КИИ)

Таблица 2

Код и наименование компетенций, формируемые с участием дисциплины	**Планируемые результаты обучения (индикаторы)**
ПК 3. Способен проводить экспертизу при расследовании компьютерных преступлений, правонарушений и инцидентов	З-1 Принципы построения компьютерных систем и сетей З-2 Уязвимости компьютерных систем и сетей З-3 Криптографические методы защиты информации З-4 Принципы построения систем управления базами данных З-5 Средства анализа конфигураций З-6 Национальные, межгосударственные и международные стандарты в области защиты информации З-7 Нормативные правовые акты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации З-9 Организационные меры по защите информации У-1

	Анализировать компьютерную систему с целью определения уровня защищенности и доверия У-2 Прогнозировать возможные пути развития действий нарушителя информационной безопасности У-3 Производить анализ политики безопасности на предмет адекватности У-4 Проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах У-5 Составлять и оформлять аналитический отчет по результатам проведенного анализа У-6 Разрабатывать предложения по устранению выявленных уязвимостей П-1 Определение уровня защищенности и доверия в компьютерных системах П-2 Оценка рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем П-3 Оценка соответствия механизмов безопасности компьютерной системы требованиям существующих нормативных документов, а также их адекватности существующим рискам П-4 Подготовка аналитического отчета по результатам проведенного анализа П-5 Формулирование предложений по устранению выявленных уязвимостей

5. ВИДЫ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ, ВКЛЮЧАЯ МЕРОПРИЯТИЯ ТЕКУЩЕЙ АТТЕСТАЦИИ

5.1. Распределение объема времени по видам учебной работы

Таблица 2

№ п/п	Наименование дисциплины модуля	Объем времени, отведенный на освоение дисциплины модуля								
		Аудиторные занятия, час.				Промежуточная аттестация (форма итогового контроля /час.)	Контактная работа (час.)	Самостоятельная работа студента, включая текущую аттестацию (час.)	Всего по дисциплине	
		Занятия лекционного типа	Практические занятия	Лабораторные работы	Всего				Час.	Зач. ед.
1	2	3	4	5	6	7	8	9	10	11
2.	Реагирование и ликвидация последствий компьютерных инцидентов в рамках функционирования центров мониторинга ГосСОПКА	36		18	54	Э	64,35	45,65	108	3
Всего на освоение дисциплины модуля (час.)		18		36	54	З	64,35	45,65	108	3

5.2. Виды СРС, количество и объем времени на контрольно-оценочные мероприятия СРС по дисциплине

Контрольно-оценочные мероприятия СРС включают самостоятельное изучение материала, подготовку к аудиторным занятиям и мероприятиям текущего контроля, выполнение и оформление внеаудиторных мероприятий текущего контроля и подготовку к мероприятиям промежуточного контроля.

Таблица 3

№ п/п	Вид самостоятельной работы студента по дисциплине модуля	Количество контрольно-оценочных мероприятий СРС	Объем контрольно-оценочных мероприятий СРС (час.)
1.	*Подготовка к лекционным*	*6*	*10 час.*
2	*Подготовка к практическим занятиям*	*16*	*16 час.*
3.	*Самостоятельное изучение материала*		*15,65*

	Подготовка к зачету	1	8 час.
		Итого на СРС по дисциплине:	45,65 *час.*

6. КРИТЕРИИ И УРОВНИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ МОДУЛЯ

3.1 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.
Личностные качества	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.

3.2 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

7. СОДЕРЖАНИЕ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ПРОМЕЖУТОЧНОГО КОНТРОЛЯ ДИСЦИПЛИНЕ МОДУЛЯ

Зачет в форме итогового тестирования с использованием ОК при реализации модели исключительно электронного обучения с использованием внутреннего онлайн-курса (ОК) УрФУ : http://courses.openedu.urfu.ru/courses/course-v1:UrFU+AOVZ+spring_2018/info

Теоретические вопросы:

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.

15. Формирование отчетных таблиц в СУБД Oracle.

Практические вопросы:

1. Создайте и продемонстрируйте работоспособность сигнатуры обнаружения атаки XSS с помощью Cisco IDS Sensor.

2. Произвести настройку сетевых интерфейсов комплекса Cisco MARS.

3. Произвести обнаружение компьютерных атак на узлы сети с использованием COA Cisco Security Agent и Cisco MARS, в результате проигранного дампа сетевого трафика.

4. Произвести установку и настройку Malcom.

5. Произвести захват и анализ проигранного дампа сетевого трафика Vulnerability № 4 с помощью Malcom.

6. Произвести анализ конфигурации узлов сети с помощью Malcom.

7. Создать отчет с отступом, 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.

8. 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.

9. 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».

10. Вывести идентификаторы атак, их наименования и оценку уязвимости всех атак при условии, что уровни опасности превышают средний и атаки зафиксированы в одной организации с любой атакой, содержащей подстроку «Bash» в поле «наименование атаки».

11. Написать запрос для вывода общего количества атак и число атак, зафиксированных ночью (с 00:00 до 06:00), утром (с 06:00 до 12:00), днем (с 12:00 до 18:00) и вечером (с 18:00 до 24:00). Дать соответствующие заголовки столбцам.

12. 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.

13. Написать запрос для вывода следующих данных о 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, общее количество атак независимо от идентификатора сети. 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 ROLLUP. 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.

15. Используя GROUPING SETS, написать запрос для вывода данных по следующим группировкам: Victim_ID, Administrator_ID, Network_ID; Victim_ID, Network_ID; Administrator_ID, Network_ID. Запрос должен подсчитывать количество атак для каждой такой группы.

Раздел 3. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ 3

Эксплуатация систем обнаружения компьютерных атак на объектах КИИ

Модуль *Обнаружение и предупреждение компьютерных атак на объектах критической информационной инфраструктуры (КИИ)*

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Коллеров Андрей Сергеевич	К.т.н.,	доцент	*Учебно-научный центр «Информационная безопасность»*

2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ *Организация защищенных сетевых коммуникаций в ИСПДн, ГИС и на объектах КИИ*

Таблица 2

Код и наименование компетенций, формируемые с участием дисциплины	**Планируемые результаты обучения (индикаторы)**
ПК 3. Способен проводить экспертизу при расследовании компьютерных преступлений, правонарушений и инцидентов.	З-1 Принципы построения компьютерных систем и сетей З-2 Уязвимости компьютерных систем и сетей З-3 Криптографические методы защиты информации З-4 Принципы построения систем управления базами данных З-5 Средства анализа конфигураций З-6 Национальные, межгосударственные и международные стандарты в области защиты информации З-7 Нормативные правовые акты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации З-9 Организационные меры по защите информации У-1

	Анализировать компьютерную систему с целью определения уровня защищенности и доверия У-2 Прогнозировать возможные пути развития действий нарушителя информационной безопасности У-3 Производить анализ политики безопасности на предмет адекватности У-4 Проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах У-5 Составлять и оформлять аналитический отчет по результатам проведенного анализа У-6 Разрабатывать предложения по устранению выявленных уязвимостей П-1 Определение уровня защищенности и доверия в компьютерных системах П-2 Оценка рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем П-3 Оценка соответствия механизмов безопасности компьютерной системы требованиям существующих нормативных документов, а также их адекватности существующим рискам П-4 Подготовка аналитического отчета по результатам проведенного анализа П-5 Формулирование предложений по устранению выявленных уязвимостей

8. ВИДЫ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ, ВКЛЮЧАЯ МЕРОПРИЯТИЯ ТЕКУЩЕЙ АТТЕСТАЦИИ

8.1. Распределение объема времени по видам учебной работы

Таблица 2

№ п/п	Наименование дисциплины модуля	Объем времени, отведенный на освоение дисциплины модуля								
		Аудиторные занятия, час.				Промежуточная аттестация (форма итогового контроля /час.)	Контактная работа (час.)	Самостоятельная работа студента, включая текущую аттестацию (час.)	Всего по дисциплине	
		Занятия лекционного типа	Практические занятия	Лабораторные работы	Всего				Час.	Зач. ед.
1	2	3	4	5	6	7	8	9	10	11
3.	Экспертно-аналитическая деятельность в центрах мониторинга ГосСОПКА	36		18	54	Э	64,35	45,65	108	3
Всего на освоение дисциплины модуля (час.)		18		36	54	З	64,35	45,65	108	3

8.2. Виды СРС, количество и объем времени на контрольно-оценочные мероприятия СРС по дисциплине

Контрольно-оценочные мероприятия СРС включают самостоятельное изучение материала, подготовку к аудиторным занятиям и мероприятиям текущего контроля, выполнение и оформление внеаудиторных мероприятий текущего контроля и подготовку к мероприятиям промежуточного контроля.

Таблица 3

№ п/п	Вид самостоятельной работы студента по дисциплине модуля	Количество контрольно-оценочных мероприятий СРС	Объем контрольно-оценочных мероприятий СРС (час.)
1.	*Подготовка к лекционным*	*6*	*10 час.*
2	*Подготовка к практическим занятиям*	*16*	*16 час.*
3.	*Самостоятельное изучение материала*		*15,65*
	Подготовка к зачету	1	8 час.
	Итого на СРС по дисциплине:		45,65 *час.*

9. КРИТЕРИИ И УРОВНИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ МОДУЛЯ

3.1 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.
Личностные качества	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.

3.2 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

10. СОДЕРЖАНИЕ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ПРОМЕЖУТОЧНОГО КОНТРОЛЯ ДИСЦИПЛИНЕ МОДУЛЯ

Зачет в форме итогового тестирования с использованием ОК при реализации модели исключительно электронного обучения с использованием внутреннего онлайн-курса (ОК) УрФУ : http://courses.openedu.urfu.ru/courses/course-v1:UrFU+AOVZ+spring_2018/info

Спецификация теста в системе ОК УрФУ:

Теоретические вопросы:

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.

Практические вопросы:

1. Произвести обнаружение компьютерных атак на узлы сети с использованием комплекса Cisco IDS Sensor.

2. Произвести обнаружение компьютерных атак на узлы сети с использованием комплекса Cisco MARS.

3. Произвести обнаружение компьютерных атак на узлы сети с использованием COA Cisco Security Agent и Cisco MARS.

4. Произвести установку и настройку Malcom.

5. Произвести захват и анализ проигранного дампа сетевого трафика Vulnerability с помощью Malcom.

6. Произвести анализ конфигурации узлов сети с помощью Malcom.

7. Создать отчет с отступом, 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.

8. 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.

9. 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» .

10. Вывести идентификаторы атак, их наименования и оценку уязвимости всех атак при условии, что уровни опасности превышают средний и атаки зафиксированы в одной организации с любой атакой, содержащей подстроку «Bash» в поле «наименование атаки».

11. Написать запрос для вывода общего количества атак и число атак зафиксированных ночью (с 00:00 до 06:00), утром (с 06:00 до 12:00), днем (с 12:00 до 18:00) и вечером (с 18:00 до 24:00). Дать соответствующие заголовки столбцам.

12. 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.

13. Написать запрос для вывода следующих данных о 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, общее количество атак независимо от идентификатора сети. 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 ROLLUP. 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.

15. Используя GROUPING SETS, Написать запрос для вывода данных по следующим группировкам: Victim_ID, Administrator_ID, Network_ID; Victim_ID, Network_ID; Administrator_ID, Network_ID. Запрос должен подсчитывать количество атак для каждой такой группы.