ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ПО ДИСЦИПЛИНЕ

Анализ событий безопасности и обеспечение функционирования технических средств сегмента 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

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 Анализ событий безопасности и обеспечение функционирования технических средств сегмента ГосСОПКА

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

2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ Анализ событий безопасности и обеспечение функционирования технических средств сегмента 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-1 - Различать стандарты ЕСКД, ЕСТД и ЕСПД З-2 - Использовать современные информационные технологии (операционные системы, базы данных, вычислительные сети) З-3 - Использовать способы реализации несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах	Домашняя работа Зачет Контрольная работа Лабораторные занятия Лекции

	З-4 - Различать основные классы и виды уязвимостей программного обеспечения З-9 - Различать методики контроля защищенности информации от несанкционированного доступа П-1 - Разрабатывать технический (эскизный) проект программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее П-2 - Испытывать программно-технические средства защиты информации от несанкционированного 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-2 - Разрабатывать проектно-сметную документацию 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 – зачет **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)		
№	**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. 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. Анализ уязвимости типа «Подделка HTTP-запросов»
2. Анализ уязвимости типа «Внедрение команд»
3. Анализ уязвимости типа «Обход директории
4. Анализ уязвимости типа «Выполнение команд на сервере
5. Анализ уязвимости типа «Внедрение операторов SQL»
6. Анализ уязвимости АСУТП
7. Нагрузочное тестирование web-сервера
8. Получение информации об актуальных компьютерных атаках из баз данных уязвимостей компьютерных систем
9. Установка и настройка COA Snort
10. Создание правил COA Snort

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. Уязвимости компьютерных систем и сетевые атаки.
2. Архитектура и принципы работы систем обнаружения атак.
3. Нормативные требования в области ГосСОПКА.
4. Обнаружение вторжений в сети с помощью средств с открытым кодом.
5. Анализ уязвимостей

Примерные задания

1. Отметьте правильный ответ

Данная техника заключается в создании специального iFrame с помощью CSS и Javascript, которые создает кнопку-подделку, по нажатию (или автоматически, без действия пользователя) на которую в невидимый iframe загрузится специальная страница с вредоносным кодом.

1) AXFR;
1) SQL Injection;
2) Remote File Inclusion;
3) Clickjacking.

2. Отметьте правильный ответ

Данная техника атак направлена на получение доступа к файлам, директориям и командам, находящимся вне основной директории Веб-сервера. Злоумышленник может манипулировать параметрами URL с целью получить доступ к файлам или выполнить команды, располагаемые в файловой системе Веб-сервера.

1) Path Traversal;
4) SQL Injection;
5) Remote File Inclusion;
6) Clickjacking.

3. Отметьте правильный ответ

Атаки данного класса направлены на получение дополнительной информации о Веб-приложении. Используя эти уязвимости, злоумышленник может определить используемые дистрибутивы ПО, номера версий клиента и сервера и установленные обновления.

1) Information Disclosure;
7) Information Leakage;
8) Credential/Session Prediction;
9) Clickjacking.

4. Отметьте правильный ответ

Эти уязвимости возникают в ситуациях, когда сервер публикует важную информацию, например, комментарии разработчиков или сообщения об ошибках, которая может быть использована для компрометации системы.

1) Information Disclosure;
10) Information Leakage;
11) Credential/Session Prediction;
12) Clickjacking.

5. Отметьте правильный ответ

Предсказуемое значение идентификатора сессии, которое позволяет перехватывать сессии других пользователей?

1) Information Disclosure;
13) Information Leakage;
14) Credential/Session Prediction;
15) Clickjacking.

LMS-платформа − не предусмотрена

5.2.2. Домашняя работа

Примерный перечень тем

1. Провести установку, настройку программного обеспечения для обнаружения эксплуатации уязвимостей

Примерные задания

1. Произвести установку и настройку COA
2. Произвести нагрузочное тестирование web-сервера
3. Создать правило COA для обнаружения эксплуатации уязвимости типа «Подделка HTTP-запросов».
4. Создать правило COA для обнаружения эксплуатации уязвимости типа «Внедрение команд».
5. Создать правило COA для обнаружения эксплуатации уязвимости типа «Обход директории».
6. Создать правило COA для обнаружения эксплуатации уязвимости типа «Выполнение команд на сервере».
7. Создать правило COA для обнаружения эксплуатации уязвимости типа «Внедрение операторов SQL».
8. Оформить отчет по домашней работе

LMS-платформа − не предусмотрена

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

5.3.1. Зачет

Список примерных вопросов

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.
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.