ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ПО ДИСЦИПЛИНЕ

Эксплуатация систем обнаружения компьютерных атак на объектах 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	Гибилинда Роман Владимирович	кандидат технических наук, без ученого звания	Доцент	
2	Коллеров Андрей Сергеевич	к.т.н., доцент	доцент	УНЦ ИБ
3	Пономарева Ольга Алексеевна	-, -	старший преподаватель	УНЦ ИБ

Согласовано:

Управление образовательных программ Т.Г. Комарова

Авторы:

- **Гибилинда Роман Владимирович, Доцент,**
- **Коллеров Андрей Сергеевич, доцент, УНЦ ИБ**
- **Пономарева Ольга Алексеевна, старший преподаватель, УНЦ ИБ**

1. СТРУКТУРА И ОБЪЕМ ДИСЦИПЛИНЫ Эксплуатация систем обнаружения компьютерных атак на объектах КИИ

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 Эксплуатация систем обнаружения компьютерных атак на объектах 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-1 - Различать стандарты ЕСКД, ЕСТД и ЕСПД З-10 - Различать средства проектирования электронных схем 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	Домашняя работа Зачет Контрольная работа Лабораторные занятия Лекции

	информацию и ее носители в автоматизированных системах З-4 - Различать основные классы и виды уязвимостей программного обеспечения З-6 - Использовать программные (программно-технические) средства защиты автоматизированных систем от несанкционированного доступа к информации и специальных программных воздействий на нее З-8 - Использовать средства 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 П-4 - Применять информацию от несанкционированного доступа и специальных воздействий на нее 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 – 0.50		
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 – 0.5		
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 –0.50		
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		
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. Захват и анализ сетевого трафика с использованием анализатора WireShark
2. Изучение механизма работы Web-уязвимостей с использованием интерактивного учебника
3. Создание простых правил системы обнаружения атак Snort
4. Поиск компьютерных атак на Web-приложения в сетевом трафике с созданием правил СОА Snort
5. Поиск комплексных компьютерных атак в сетевом трафике с созданием правил СОА Snort
6. Поиск и устранение уязвимостей Web-приложений
7. Создание правил СОА Snort на основе эксплуатации сетевых и Web-уязвимостей
8. Работа с базами данных правил СОА
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. Проектирование SIEM (Security information and event management) системы на основе системы обнаружения компьютерных атак Snort для применения на объекте КИИ
2. Проектирование SIEM (Security information and event management) системы на основе системы обнаружения компьютерных атак Suricata для применения на объекте КИИ
3. Проектирование сегмента сети объекта КИИ с установкой и настройкой СОКА и SIEM
4. Категорирование объекта КИИ и требования по безопасности КИИ.
5. Определение компьютерной атаки. Классификация компьютерных атак. Базы данных уязвимостей.
6. Инвентаризация узлов сети.

Примерные задания
1. Отметьте правильные ответы
Элементами HTTP-заголовка запроса к серверу являются:
а) Accept;
б) User-Agent;
в) Content-Type;
г) Content-Length:.

2. Отметьте правильные ответы
Элементами HTTP-заголовка ответа сервера являются:
а) Accept;
б) User-Agent;
в) Content-Type;
г) Content-Length.

3. Отметьте правильный ответ
Код HTTP-ответа сервера вида 4xx:
а) указывает на ошибку на стороне сервера;
б) указывает на то, что запрос успешно обработан;
в) указывает на ошибку на стороне клиента;
г) указывает на перенаправление запроса.

4. Отметьте правильный ответ
Код HTTP-ответа сервера вида 5xx:
а) указывает на ошибку на стороне сервера;
б) указывает на то, что запрос успешно обработан;
в) указывает на ошибку на стороне клиента;
г) указывает на перенаправление запроса.

5. Отметьте правильные ответы
GET-запрос в протоколе HTTP является:
а) идемпотентным (idempotent);
б) безопасным (safe);
в) неидемпотентным (non-idempotent);
г) небезопасным (not safe).

6. Отметьте правильные ответы
POST-запрос в протоколе HTTP является:
а) идемпотентным (idempotent);
б) безопасным (safe);
в) неидемпотентным (non-idempotent);
г) небезопасным (not safe).

7. Отметьте правильные ответы
PUT-запрос в протоколе HTTP является:
а) идемпотентным (idempotent);
б) безопасным (safe);
в) неидемпотентным (non-idempotent);
г) небезопасным (not safe).

8. Дополните утверждение
Cookies — это…
а) небольшой объём данных, присланный сервером браузеру и хранимый на диске;
б) механизм управления сроком хранения документов в кэше;
в) механизм авторизации;
г) поле данных HTTP-пакета.

9. Отметьте правильный ответ
Какой тип запроса должен выполняться при аутентификации пользователя?

а) GET;
б) PUT;
в) POST;
г) GOT.

10. Отметьте правильные ответы
Что означает флаг secure, установленный для cookies?
а) запрос только по HTTPS;
б) запрос только по HTTP;
в) не доступны через JS;
г) доступны через JS.

11. Дополните утверждение
Одно из ключевых понятий протокола OAuth — это…
а) access token;
б) private key;
в) foreign key;
г) basic token.

12. Отметьте правильные ответы
Укажите правильно составленный URL
а) http://mail.ru;
б) simple@email.com;
в) data:image/gifbase64,R0lGODlhEAAOALMAAOazToeHh0tLS;
г) ftp://haker\:h_keR@nowhere.com/.

13. Отметьте правильные ответы
Укажите правильно составленный URI
а) http\://mail.ru;
б) simple@email.com;
в) data\:image/gifbase64,R0lGODlhEAAOALMAAOazToeHh0tLS;
г) ftp\://haker\:h_keR@nowhere.com/.

14. Отметьте правильные ответы
На каких протоколах основывается сервис передачи файлов?
а) smtp;
б) pop3;
в) ftp;
г) http.

15. Отметьте правильный ответ
HTTP-заголовок "Authorization: Basic ..." является…
а) заголовком запроса к серверу;

б) заголовком ответа сервера;
в) является некорректным.

LMS-платформа − не предусмотрена

5.2.2. Домашняя работа

Примерный перечень тем

1. Разработка правил на обнаружение в сетевом трафике атак

Примерные задания

1. Подготовка сетевого трафика для анализа.
2. Создать правила на обнаружение в сетевом трафике строковых сигнатур
3. Создать правила на обнаружение в сетевом трафике двоичных сигнатур.
4. Создать правила на обнаружение в сетевом трафике атаки типа XSS в поле URI заголовка HTTP
5. Создать правила на обнаружение в сетевом трафике атаки типа SQL injection в теле POST-запроса пакета протокола HTTP
6. Создать правила на обнаружение в сетевом трафике атаки типа Command injection в поле URI заголовка HTTP для операционных систем на базе ядра Linux
7. 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. Основные положения Федерального закона № 187-ФЗ
2. Категорирование объекта КИИ
3. Требования по безопасности КИИ
4. Определение компьютерной атаки. Классификация компьютерных атак. Базы данных уязвимостей.
5. Инвентаризация узлов сети.
6. Атаки типа «Отказ в обслуживании» (Denial of Service).
7. Атаки на прикладное программное обеспечение.
8. Атаки на уязвимости Web-приложений.
9. Определение системы обнаружения атак. Сигнатурный анализ и обнаружение аномалий.
10. Обнаружение атак в реальном времени и отложенный анализ.
11. Локальные и сетевые системы обнаружения атак.
12. Распределенные системы обнаружения атак.
13. Многоагентные системы обнаружения атак.
14. Общие сведения о Snort. Установка и запуск.
15. Описание языка правил Snort.
16. Использование COA Snort.
17. Использование препроцессоров COA Snort.

18. Общие сведения о СОА Suricata. Установка и настройка.

19. Использование СОА Suricata.

20. Назначение СОА Cisco IDS Sensor.

21. Назначение СОА Cisco IDS Sensor. Варианты современных подходов к решению задачи обнаружения аномалий, использующие нейросетевые решения.

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.