Приложение к рабочей программе дисциплины (практики)

Федеральное государственное автономное образовательное учреждение высшего образования «Российский университет дружбы народов имени Патриса Лумумбы» (РУДН)

Факультет искусственного интеллекта

(наименование основного учебного подразделения)

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ И СИСТЕМА ОЦЕНИВАНИЯ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ ПО ДИСЦИПЛИНЕ (ПРАКТИКЕ)

СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

(наименование дисциплины (практики))

Оценочные материалы рекомендованы МССН для направления подготовки/ специальности:

10.04.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

(код и наименование направления подготовки/ специальности)

Освоение дисциплины (практики) ведется в рамках реализации основной профессиональной образовательной программы (ОП ВО, профиль/ специализация):

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

(направленность (профиль) ОП ВО)

Москва, 2025

1. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ПО ДИСЦИПЛИНЕ (ПРАКТИКЕ)

Перечень вопросов, заданий, тем для подготовки к текущему контролю

Основные формы текущего контроля знаний:

- выступление с докладом по проблемным темам дисциплины;
- собеседование по теоретическим вопросам;
- решение ситуационных задач;
- выполнение учебных практических заданий (лабораторных работ);
- выполнение аудиторных самостоятельных работ, контрольных работ, обсуждение и анализ их результатов;

Примерный перечень вопросов к контрольной работе

1. Классификация аномалий в IP-сетях.
2. Классификация атак в киберсреде и типичные этапы их реализации.
3. Методы и средства повышения функциональности хостовых датчиков.
4. Проблема ложных срабатываний и обеспечение корреляции событий в системах обнаружения вторжений.
5. Повышение производительности СОВ для работы в гигабайтных сетях.
6. Повышение отказоустойчивости системы с целью недопущения снижения доступности к критическим приложениям.
7. Поддержка новых технологий и протоколов для противодействия атакам на прикладном уровне.
8. Решение проблемы кооперации систем обнаружения вторжений разных производителей в рамках одной инфраструктуры предотвращения атак.
9. Эксплуатационные функции систем обнаружения вторжений и организационно-технологические приложения их реализации.
10. Виды управленческих решений при функционировании систем обнаружения вторжений.

В течении семестра студент может набрать максимальное количество баллов равное 40. На промежуточную аттестацию отводится 60 баллов. Распределение баллов по видам работ, формирующих текущий контроль успеваемости по дисциплине, отражает качество подготовки обучающихся к занятиям семинарского типа и выполнение различных видов самостоятельных работы.

Критерии балльной оценки различных форм текущего контроля успеваемости содержатся в соответствующих методических рекомендациях Департамента информационной безопасности.

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Перечень компетенций, формируемых в процессе освоения дисциплины

Перечень компетенций, формируемых в процессе освоения дисциплины содержится в Разделе 2. «Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине».

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, владений.

Таблица 5

Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами	Типовые контрольные задания

		достижения компетенции	
ОПК-3 Способен использовать необходимые математические методы для решения задач профессиональной деятельности	1. Демонстрирует знание основных математических методов, использующихся в области информационной безопасности.	1. Знать основные математические методы кодирования и декодирования. 2. Уметь решать типовые для информационной безопасности задачи кодирования и декодирования	**Задание 1.** Перечислите основные механизмы помехоустойчивого кодирования. **Задание 2.** Опишите в общем виде алгоритм вычисления CRC.
	2. Демонстрирует умение осуществлять выбор эффективных математических методов для решения задач профессиональной деятельности	1. Знать эффективные методы кодирования и декодирования 2. Уметь выбирать эффективные методы кодирования и декодирования в задачах информационной безопасности	**Задание 1.** В чем состоит концепция линейного сетевого кодирования? Каково ее применение в современных сетях? **Задание 2.** Опишите механизм проверки ошибок в TCP/UDP пакетах. Чем обоснован такой механизм? Как его можно было бы улучшить?
	3. Показывает владение навыками применения основных математических методов в задачах информационной безопасности	1. Знать способы применения методов кодирования и декодирования в задачах информационной безопасности. 2. Уметь применять методы кодирования и декодирования в	**Задание 1.** Разберите следующий дамп: 0x0000: 0050 569c 35a3 0000 0000 0000 0800 4600 .PV.5.....F. 0x0010: 0024 0000 0000 0102 3ad3 0a00 0000 e000 .$.....:..... 0x0020: 0001 9404 0000 1101 ebfe 0000 0000 0300 ..... 0x0030: 0000 0000 0000 0000 0000 0000 ..... Ответьте на вопросы: Какой протокол используется? Каковы параметры этого протокола? Какой IP исходящего пакета? **Задание 2.**

		задачах информационной безопасности.	Разберите следующий дамп: 0x0000: 4500 0034 0014 0000 2e06 c005 4e8e d16e E..4.....N..n 0x0010: ac1e 0090 6c86 01bb 8e0a b73e 1095 9779 ....l.....>...y 0x0020: 8010 001c d202 0000 0101 080a 3803 7b55 ....8.{U 0x0030: 4801 8100 Ответьте на вопросы: Какой протокол используется? Какой исходящий порт и какой порт назначения? Какие флаги установлены?
ОПК-4.3 Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных финансово-банковских систем;	1. Устанавливает программные, программно-аппаратные, в том числе криптографические и технические средства защиты информации автоматизированных систем. 2. Тестирует и настраивает программные, программно-аппаратные, в том числе криптографические и технические средства защиты информации автоматизированных систем	1. Знать методы и способы установки программного, программно-аппаратного обеспечения средств защиты автоматизированных систем. 2. Уметь устанавливать программные, программно-аппаратные средства защиты информации автоматизированных систем. 1. Знать способы тестирования программно-аппаратных средств защиты информации. 2. Уметь определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы;	**Задание 1.** Перечислите основные механизмы интеграция компонентов системы обнаружения вторжений. **Задание 2.** Напишите алгоритм установки ПО Snort и сопутствующего ПО на систему Astra Linux. **Задание 1.** Перечислите типовые причины отказов сетевых СОВ в зависимости от их типа. **Задание 2.** Перечислите типовые причины отказов хостовых СОВ.

ОПК - 4.4 Способен осуществлять диагностику и мониторинг систем защиты автоматизированных финансово-банковских систем;	1. Диагностирует состояние систем защиты автоматизированных систем на основании анализа данных мониторинга систем защиты информации и принимает оперативные решения о состоянии защищенности информационной системы. 2. Эффективно выбирает системы мониторинга защиты автоматизированных систем. 3. Устанавливает и конфигурирует системы мониторинга защиты автоматизированных систем.	1. Знает методы диагностирования состояния систем защиты на основании анализа данных мониторинга систем защиты информации. 2. Уметь обнаруживать и идентифицировать инциденты в процессе эксплуатации автоматизированной системы; методами оценки защищенности автоматизированных систем с помощью типовых программных средств. 1. Знает эффективные механизмы выбора системы мониторинга защиты информации. 2. Умеет эффективно выбирать системы мониторинга защиты автоматизированных систем.	**Задание 1.** Перечислите основные документы ФСТЭК регламентирующие контроль защиты информации. **Задание 2.** Перечислите основные (на сегодняшний день) причины возникновения инцидентов информационной безопасности. **Задание 1.** Какие отечественные СОВ уровня сети можно применять для значимых объектов КИИ 1 категории. Перечислите возможные варианты. Выберите один с обоснованием. **Задание 2.** Ваша организация является оператором персональных данных и содержит значимые объекты КИИ 1й категории. Выберите СОВ уровня узла, ответ обоснуйте. **Задание 1.** Рассмотрите следующий трафик (ответы не показаны): 13:21:45.010117 holmes.4033 > watson.220: S 93266:93266(0) win 8192

		1. Знает способы конфигурирования систем мониторинга защиты информации автоматизированных систем. 2. Умеет устанавливать и конфигурировать системы мониторинга защиты автоматизированных систем.	13:21:45.011128 holmes.4003 > watson.ftp: S 92918:92918(0) win 8192 13:21:45.012014 holmes.4005 > watson.telnet: S 92946:92946(0) win 8192 13:21:45.013095 holmes.4004 > watson.22: S 92932:92932(0) win 8192 13:21:45.014107 holmes.4019 > watson.110: S 93094:93094(0) win 8192 13:21:45.015865 holmes.4010 > watson.63: S 93016:93016(0) win 8192 13:21:45.016763 holmes.4021 > watson.nntp: S 93106:93106(0) win 8192 13:21:45.018001 holmes.4016 > watson.80: S 93076:93076(0) win 8192 13:21:45.018456 holmes.4017 > watson.92: S 93154:93154(0) win 8192 13:21:45.018997 holmes.4034 > watson.396: S 93280:93280(0) win 8192 13:21:45.019562 holmes.4031 > watson.215: S 93238:93238(0) win 8192 13:21:45.020017 holmes.4002 > watson.17: S 92912:92912(0) win 8192 Что пытается узнать систем holmes? Является ли данное событие инцидентом безопасности? Как нужно сконфигурировать СОВ для предотвращения этого события? **Задание 2.** Перечислите аргументы за и против блокирования протокола ICMP при конфигурировании СОВ уровня сети.

Примерный перечень вопросов для проверки уровня компетенций

1. Система обнаружения вторжений. Понятие. Функции.

2. Программные и программно-аппаратные средства обнаружения вторжений.

3. Признаки атаки и жизненный цикл вторжения в автоматизированную систему.

4. Классы систем обнаружения вторжений и их характеристика.

5. Понятие киберпространства в информационном обществе.

6. Цели и задачи интеллектуальной системы обеспечения безопасности автоматизированной системы в финансово-кредитной и банковской сферах.

7. Цель и задачи экспериментальных исследований систем обнаружения вторжений.

8. Функция активного противодействия вторжениям.

9. Функция оперативного оповещения о вторжениях.

10. Типовая архитектура систем обнаружения вторжений.

11. Логическая структура систем обнаружения вторжений.

12. Информационный фонд системы обнаружения вторжений.

13. Назначение и функции систем обнаружения.

14. Координационный центр системы обнаружения вторжений и его функции.

15. Назначение и функции консоли администратора системы обнаружения вторжений.

16. Интеграция компонентов системы обнаружения вторжений.

17. Схема включения системы обнаружения вторжений в автоматизированную информационную систему.

18. Критерии сравнения систем обнаружения вторжений.

19. Специальный компонент «агент БД» системы обнаружения вторжений.

20. Координационный центр системы обнаружения вторжений и его функции.

21. Назначение и функции консоли администратора системы обнаружения вторжений.

22. Модули интеграции с сетевым оборудованием системы обнаружения вторжений.

23. Функции модуля интеграции с сетевым оборудованием системы обнаружения вторжений.

24. Модуль почтовых уведомлений системы обнаружения вторжений.

25. Агенты и сетевые датчики системы обнаружения вторжений.

26. Хостовые датчики системы обнаружения вторжений.

27. Интеграция компонентов системы обнаружения вторжений.

28. Схемы включения системы обнаружения вторжений в автоматизированную информационную систему.

29. Задачи администрирования системы обнаружения вторжений.

30. Опишите типовые работы по установке, настройке и обслуживанию программных, программно-аппаратных систем обнаружения вторжений.

Примеры практико-ориентированных заданий

Задача1. Разработайте инструкцию администратора системы обнаружения вторжений.

Задача 2. Предложите критерии сравнения и проведите сравнительную оценку нескольких систем обнаружения вторжений.

Задача 3. Разработайте схему процесса реализации вторжения внешнего нарушителя в банковскую автоматизированную систему.

Задача 4. Проведите первоначальную настройку системы обнаружения MaxPatrol.

Задача 5. В журнале системы обнаружения вторжения вы наблюдаете следующий трафик:

1 11:47:50.047936 altamont.champlain.edu.4490 > ns.champlain.edu.53: 37273+ A? ftp.example.net. (33)
2 1:47:50.048450 ns.champlain.edu.53 > altamont.champlain.edu.4490: 37273 1/3/0 A 209.198.87.45 (106)
3 11:47:50.881828 altamont.champlain.edu.1074 > ftp.example.net.21: S 1704258988:1704258988(0) win 65535 <mss 1460,nop,nop,sackOK>
4 11:47:50.937928 ftp.example.net.21 > altamont.champlain.edu.1074: S 3565913320:3565913320(0) ack 1704258989 win 8760 <mss 1460>
5 11:47:50.938011 altamont.champlain.edu.1074 > ftp.example.net.21: . ack 1 win 65535
6 11:47:51.764584 ftp.example.net.21 > altamont.champlain.edu.1074: P 1:65(64) ack 1 win 8760
7 11:47:51.926930 altamont.champlain.edu.1074 > ftp.example.net.21: . ack 65 win 65471
8 11:47:57.478597 altamont.champlain.edu.1074 > ftp.example.net.21: P 1:17(16) ack 65 win 65471
9 11:47:57.506130 ftp.example.net.21 > altamont.champlain.edu.1074: P 65:123(58) ack 17 win 8760
: :
: :
: :
10 11:48:19.215466 ftp.example.net.21 > altamont.champlain.edu.1074: F 421:421(0) ack 123 win 8760
11 11:48:19.215555 altamont.champlain.edu.1074 > ftp.example.net.21: . ack 422 win 65115

12 11:48:19.220559 altamont.champlain.edu.1074 > ftp.example.net.21: F 123:123(0) ack 422 win 65115
13 11:48:19.296084 ftp.example.net.21 > altamont.champlain.edu.1074: . ack 124 win 8760

Опишите сценарий того, что происходит.