Приложение 4

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное автономное
образовательное учреждение высшего образования
«Национальный исследовательский Нижегородский государственный университет
им. Н.И. Лобачевского»

Радиофизический факультет

УТВЕРЖДЕНО

решением президиума Ученого совета ННГУ

протокол № 1 от 16.01.2024 г.

Рабочая программа дисциплины

Методы обнаружения сетевых аномалий

Уровень высшего образования
Специалитет

Направление подготовки / специальность
10.05.02 - Информационная безопасность телекоммуникационных систем

Направленность образовательной программы
Системы подвижной цифровой защищенной связи

Форма обучения
очная

г. Нижний Новгород

2024 год начала подготовки

1. Место дисциплины в структуре ОПОП

Дисциплина Б1.О.42 Методы обнаружения сетевых аномалий относится к обязательной части образовательной программы.

2. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями и индикаторами достижения компетенций)

Формируемые компетенции (код, содержание компетенции)	**Планируемые результаты обучения по дисциплине (модулю), в соответствии с индикатором достижения компетенции**		**Наименование оценочного средства**	
	Индикатор достижения компетенции (код, содержание индикатора)	**Результаты обучения по дисциплине**	**Для текущего контроля успеваемости**	**Для промежуточной аттестации**
ОПК-15: Способен проводить инструментальный мониторинг качества обслуживания и анализ защищенности информации от несанкционированного доступа в телекоммуникационных системах и сетях в целях управления их функционированием ;	*ОПК-15.1: Знает: - методики измерения и оценки параметров в телекоммуникационных системах ОПК-15.2: Умеет: - проводить измерения в спектральной и временной области - анализировать пропускную способность и предельную нагрузку сети связи - анализировать параметры передачи кадров при прохождении по каналам связи - проверять достижимость абонентов сети связи - выявлять трафик сетевых атак*	*ОПК-15.1: Знать: - методики измерения и оценки параметров в телекоммуникационных системах ОПК-15.2: Уметь: - проводить измерения в спектральной и временной области - анализировать пропускную способность и предельную нагрузку сети связи - анализировать параметры передачи кадров при прохождении по каналам связи - проверять достижимость абонентов сети связи - выявлять трафик сетевых атак*	*Собеседование*	*Зачёт: Контрольные вопросы*

3. Структура и содержание дисциплины

3.1 Трудоемкость дисциплины

	очная
Общая трудоемкость, з.е.	**3**
Часов по учебному плану	**108**
в том числе	
аудиторные занятия (контактная работа):	
- занятия лекционного типа	**0**

- занятия семинарского типа (практические занятия / лабораторные работы)	**64**
- КСР	**1**
самостоятельная работа	**43**
Промежуточная аттестация	**0** **Зачёт**

3.2. Содержание дисциплины

(структурированное по темам (разделам) с указанием отведенного на них количества академических часов и виды учебных занятий)

Наименование разделов и тем дисциплины	Всего (часы)	в том числе			
		Контактная работа (работа во взаимодействии с преподавателем), часы из них			Самостоятельная работа обучающегося, часы
		Занятия лекционного типа	Занятия семинарского типа (практические занятия/лабораторные работы), часы	Всего	
	ооо	ооо	ооо	ооо	ооо
1. Нормативная база в области информационной безопасности	22		6	6	16
2. Методы и системы обнаружения сетевых аномалий	85		58	58	27
Аттестация	0				
КСР	1			1	
Итого	108	0	64	65	43

Содержание разделов и тем дисциплины

1. Нормативная база в области информационной безопасности
2. Методы и системы обнаружения сетевых аномалий

4. Учебно-методическое обеспечение самостоятельной работы обучающихся

Самостоятельная работа обучающихся включает в себя подготовку к контрольным вопросам и заданиям для текущего контроля и промежуточной аттестации по итогам освоения дисциплины приведенным в п. 5.

Электронно-библиотечная система "Лань"
Электронно-библиотечная система "Юрайт"

5. Фонд оценочных средств для текущего контроля успеваемости и промежуточной аттестации по дисциплине (модулю)

5.1 Типовые задания, необходимые для оценки результатов обучения при проведении текущего контроля успеваемости с указанием критериев их оценивания:

5.1.1 Типовые задания (оценочное средство - Собеседование) для оценки сформированности компетенции ОПК-15:

1. Понятие атак на компьютерные сети. Классификация атак на компьютерные сети. Основные типы сетевых атак.

2. Модель атаки. Результат атаки. Этапы реализации атак. Сокрытие источника и факта атаки.

3. Средства реализации атак.

4. Требования, предъявляемые к СОА.

5. Определение политики и процедур безопасности.

6. Типовая архитектура СОА в составе сенсора, модуля управления, анализатора, набора протоколов взаимодействия и средства реагирования.

7. Варианты размещения СОА.

8. Размещение сенсоров СОА.

9. Реагирование на инциденты.

10. СОА Snort. Назначение, возможности.

Критерии оценивания (оценочное средство - Собеседование)

Оценка	Критерии оценивания
зачтено	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «удовлетворительно»
не зачтено	Хотя бы одна компетенция сформирована на уровне «неудовлетворительно» или на уровне «плохо»

5.2. Описание шкал оценивания результатов обучения по дисциплине при промежуточной аттестации

Шкала оценивания сформированности компетенций

Уровень сформированности компетенций (индикатора достижения	**плохо**	**неудовлетворительно**	**удовлетворительно**	**хорошо**	**очень хорошо**	**отлично**	**превосходно**
	не зачтено		**зачтено**				

компет							
Знания	Отсутствие знаний теоретического материала. Невозможность оценить полноту знаний вследствие отказа обучающегося от ответа	Уровень знаний ниже минимальных требований. Имели место грубые ошибки	Минимально допустимый уровень знаний. Допущено много негрубых ошибок	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько негрубых ошибок	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько несущественных ошибок	Уровень знаний в объеме, соответствующем программе подготовки. Ошибок нет.	Уровень знаний в объеме, превышающем программу подготовки.
Умения	Отсутствие минимальных умений. Невозможность оценить наличие умений вследствие отказа обучающегося от ответа	При решении стандартных задач не продемонстрированы основные умения. Имели место грубые ошибки	Продемонстрированы основные умения. Решены типовые задачи с негрубыми ошибками. Выполнены все задания, но не в полном объеме	Продемонстрированы все основные умения. Решены все основные задачи с негрубыми ошибками. Выполнены все задания в полном объеме, но некоторые с недочетами	Продемонстрированы все основные умения. Решены все основные задачи. Выполнены все задания в полном объеме, но некоторые с недочетами.	Продемонстрированы все основные умения. Решены все основные задачи с отдельными несущественными недочетами, выполнены все задания в полном объеме	Продемонстрированы все основные умения. Решены все основные задачи. Выполнены все задания, в полном объеме без недочетов
Навыки	Отсутствие базовых навыков. Невозможность оценить наличие навыков вследствие отказа обучающегося от ответа	При решении стандартных задач не продемонстрированы базовые навыки. Имели место грубые ошибки	Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами	Продемонстрированы базовые навыки при решении стандартных задач с некоторыми недочетами	Продемонстрированы базовые навыки при решении стандартных задач без ошибок и недочетов	Продемонстрированы навыки при решении нестандартных задач без ошибок и недочетов	Продемонстрирован творческий подход к решению нестандартных задач

Шкала оценивания при промежуточной аттестации

Оценка		**Уровень подготовки**
зачтено	**превосходно**	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «превосходно», продемонстрированы знания, умения, владения по соответствующим компетенциям на уровне выше предусмотренного программой
	отлично	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «отлично».
	очень хорошо	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «очень хорошо»
	хорошо	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «хорошо».
	удовлетворитель	Все компетенции (части компетенций), на формирование которых направлена

	но	дисциплина, сформированы на уровне не ниже «удовлетворительно», при этом хотя бы одна компетенция сформирована на уровне «удовлетворительно»
не зачтено	**неудовлетворительно**	Хотя бы одна компетенция сформирована на уровне «неудовлетворительно».
	плохо	Хотя бы одна компетенция сформирована на уровне «плохо»

5.3 Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения на промежуточной аттестации с указанием критериев их оценивания:

5.3.1 Типовые задания (оценочное средство - Контрольные вопросы) для оценки сформированности компетенции ОПК-15

1. Уязвимости. Классификация уязвимостей.

2. Понятие атак на компьютерные сети. Классификация атак на компьютерные сети. Основные типы сетевых атак.

3. Модель атаки. Результат атаки. Этапы реализации атак. Сокрытие источника и факта атаки.

4. Средства реализации атак.

5. Механизмы типовых атак, основанных на уязвимостях сетевых протоколов.

6. Атаки на сетевые службы. Атаки с использованием промежуточных узлов и территорий.

7. Технологии обнаружения компьютерных атак и их возможности.

8. Прямые и косвенные признаки атак. Источники информации об атаках.

9. Методы обнаружения атак. Обнаружение аномалий и обнаружение злоупотреблений. Обнаружение следов атак.

10. Классификация систем обнаружения атак (СОА). Сетевые и узловые СОА.

11. Требования, предъявляемые к СОА.

12. Системы анализа защищенности. «Классические» системы обнаружения атак и анализаторы журналов регистрации. Обманные системы. Системы контроля целостности.

13. Определение политики и процедур безопасности.

14. Генерация информации для контроля целостности системных файлов и данных.

15. Типовая архитектура СОА в составе сенсора, модуля управления, анализатора, набора протоколов взаимодействия и средства реагирования.

16. Варианты размещения СОА.

17. Размещение сенсоров СОА.

18. Размещение системы анализа защищенности.

19. Размещение системы контроля целостности.

20. Размещение обманной системы.

21. Проблемы, связанные с СОА.

22. Реагирование на инциденты.

23. СОА Snort. Назначение, возможности.

Критерии оценивания (оценочное средство - Контрольные вопросы)

Оценка	Критерии оценивания
зачтено	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «удовлетворительно»
не зачтено	Хотя бы одна компетенция сформирована на уровне «неудовлетворительно» или на уровне «плохо»

6. Учебно-методическое и информационное обеспечение дисциплины (модуля)

Основная литература:

1. Трофимов Валерий Владимирович. Глобальные и локальные сети : учебник для вузов / В. В. Трофимов, М. И. Барабанова, В. И. Кияев. - 4-е изд. - Москва : Юрайт, 2023. - 162 с. - (Высшее образование). - ISBN 978-5-534-17504-2. - Текст : электронный // ЭБС "Юрайт"., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=891846&idb=0.
2. Милославская Н. Г. Сетевые атаки на открытые системы на примере Интранета : учебное пособие для вузов / Милославская Н. Г. - Москва : НИЯУ МИФИ, 2012. - 64 с. - Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений. - Библиогр.: доступна в карточке книги, на сайте ЭБС Лань. - Книга из коллекции НИЯУ МИФИ - Информатика. - ISBN 978-5-7262-1691-1., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=716282&idb=0.
3. Технологии защиты информации в компьютерных сетях / Руденков Н.А., Пролетарский А.В., Смирнова Е.В., Суровов А.М. - Москва : ИНТУИТ, 2016., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=663523&idb=0.

Дополнительная литература:

1. Щеглов А. Ю. Защита информации: основы теории : учебник / А. Ю. Щеглов, К. А. Щеглов. - Москва : Юрайт, 2023. - 309 с. - (Высшее образование). - ISBN 978-5-534-04732-5. - Текст : электронный // ЭБС "Юрайт"., https://e-lib.unn.ru/MegaPro/UserEntry?

Action=FindDocs&ids=840752&idb=0.
2. Шелухин О. И. Искусственный интеллект и машинное обучение в кибербезопасности : учебно-методическое пособие для выполнения лабораторных работ. направление подготовки: 10.03.01 информационная безопасность. профили: «безопасность компьютерных систем», «безопасность автоматизированных систем» / Шелухин О. И.,Осин А. В.,Раковский Д. И. - Москва : МТУСИ, 2022. - 52 с. - Книга из коллекции МТУСИ - Информатика., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=865878&idb=0.

Программное обеспечение и Интернет-ресурсы (в соответствии с содержанием дисциплины):

SNORT Users Manual (https://snort.org/)

7. Материально-техническое обеспечение дисциплины (модуля)

Учебные аудитории для проведения учебных занятий, предусмотренных образовательной программой, оснащены мультимедийным оборудованием (проектор, экран), техническими средствами обучения, компьютерами.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечены доступом в электронную информационно-образовательную среду.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки/специальности 10.05.02 - Информационная безопасность телекоммуникационных систем.

Автор(ы): Ротков Леонид Юрьевич, кандидат технических наук, доцент
Нужный Роман Геннадьевич.

Заведующий кафедрой: Ротков Леонид Юрьевич, кандидат технических наук.

Программа одобрена на заседании методической комиссии от 18 декабря 2023 года, протокол № 09/23.