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
(факультет / институт / филиал)

УТВЕРЖДЕНО
решением ученого совета ННГУ
протокол от
«31» мая 2023 г. № 6

Рабочая программа дисциплины

Системы обнаружения компьютерных атак
(наименование дисциплины (модуля))

Уровень высшего образования
магистратура
(бакалавриат / магистратура / специалитет)

Направление подготовки / специальность
02.04.02 Фундаментальная информатика и информационные технологии
(указывается код и наименование направления подготовки / специальности)

Направленность образовательной программы
Информационная безопасность и защита информации
(указывается профиль / магистерская программа / специализация)

Форма обучения
очная
(очная / очно-заочная / заочная)

Нижний Новгород

2023

1. Место дисциплины в структуре ООП

Дисциплина «Системы обнаружения компьютерных атак» относится к дисциплинам части, формируемой участниками образовательных отношений, основной образовательной программы по направлению подготовки 02.04.02 «Фундаментальная информатика и информационные технологии».

№ варианта	Место дисциплины в учебном плане образовательной программы	Стандартный текст для автоматического заполнения в конструкторе РПД
2	Блок 1. Дисциплины (модули) Часть, формируемая участниками образовательных отношений	Дисциплина Б1.В.ДВ.04.01 «Системы обнаружения компьютерных атак» относится к части ООП направления подготовки 02.04.02 «Фундаментальная информатика и информационные технологии», формируемой участниками образовательных отношений.

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**	
ПК-1. Способен руководить научными исследованиями и опытно-конструкторскими разработками, в области фундаментальной информатики и информационных технологий (ФИИТ), и формировать их новые направления в области профессиональной деятельности	ПК-1.1. Знает проблематику и методы научных исследований и опытно-конструкторских разработок в области ФИИТ применительно к профессиональной деятельности	Знать: - проблематику и методы научных исследований и опытно-конструкторских разработок в области построения систем обнаружения компьютерных атак	Собеседование
	ПК-1.2. Умеет выполнять научные исследования и опытно-конструкторские разработки в области ФИИТ применительно к профессиональной деятельности.	Уметь: - выполнять научные исследования и опытно-конструкторские разработки в области построения систем обнаружения компьютерных атак	Собеседование
ПК-10. Способен применять в профессиональной деятельности	ПК-10.1. Знает стандарты, процедуры и средства администрирования и управления	Знать: - стандарты, процедуры и средства администрирования и управления безопасностью информационных технологий в области построения	Собеседование

стандарты, процедуры и средства администрирования и управления безопасностью информационных технологий; способен использовать стандарты, процессы, процедуры и средства поддержки жизненного цикла информационных технологий	безопасностью информационных технологий.	систем обнаружения компьютерных атак	
	ПК-10.2. Умеет применять в профессиональной деятельности стандарты, процедуры и средства администрирования и управления безопасностью информационных технологий.	Уметь: - применять в профессиональной деятельности стандарты, процедуры и средства администрирования и управления безопасностью информационных технологий в области построения систем обнаружения компьютерных атак	Собеседование

3. Структура и содержание дисциплины

3.1 Трудоемкость дисциплины

	очная форма обучения	**очно-заочная форма обучения**	**заочная форма обучения**
Общая трудоемкость	**3 ЗЕТ**	**___ ЗЕТ**	**___ ЗЕТ**
Часов по учебному плану	**108**		
в том числе			
аудиторные занятия (контактная работа): **- занятия лекционного типа** **- занятия семинарского типа (практические занятия / лабораторные работы)**	**32**		
самостоятельная работа	**75**		
КСР	**1**		
Промежуточная аттестация – экзамен/зачет	**зачет**		

3.2. Содержание дисциплины

Наименование и краткое содержание разделов и тем дисциплины,	**Всего (часы)**	В том числе	
		Контактная работа (работа во взаимодействии с преподавателем), часы из них	**рабо та обуч**

форма промежуточной аттестации по дисциплине		**Занятия лекционного типа**	**Занятия семинарского типа**	**Занятия лабораторного типа**	**Всего**	
1. Нормативная база в области информационной безопасности	28	6			6	22
2. Системы обнаружения компьютерных атак	79	26			26	53
Итого:	107	32			32	75

4. Учебно-методическое обеспечение самостоятельной работы обучающихся

Самостоятельная работа обучающихся включает следующие виды:

- изучение дополнительных разделов дисциплины с использованием учебной литературы;

- изучение и проверка компьютерных настроек и интерфейсов на персональных компьютерах обучающихся.

Используется учебно-методическое пособие «Настройка и эксплуатация системы обнаружения атак «Snort».

Текущий контроль усвоения материала проводится путем проведения опроса.

Контрольные вопросы и задания для проведения текущего контроля и промежуточной аттестации по итогам освоения дисциплины приведены в п. 5.2.

5. Фонд оценочных средств для промежуточной аттестации по дисциплине (модулю),

включающий:

5.1. Описание шкал оценивания результатов обучения по дисциплине

Уровень сформированности компетенций (индикатора достижения компетенций)	**Шкала оценивания сформированности компетенций**						
	не зачтено		**зачтено**				
Знания	Отсутствие знаний теоретического материала. Невозможность оценить	Уровень знаний ниже минимальных требований. Имели место грубые	Минимально допустимый уровень знаний. Допущено много негрубых	Уровень знаний в объеме, соответствующем программе подготовки.	Уровень знаний в объеме, соответствующем программе подготовки. Допущено	Уровень знаний в объеме, соответствующем программе подготовки,	Уровень знаний в объеме, превышающем программу подготовки.

	полноту знаний вследствие отказа обучающегося от ответа	ошибки.	ошибки.	Допущено несколько негрубых ошибок	несколько несущественных ошибок	без ошибок.	
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 несущественным недочетами, выполнены все задания в полном объеме.	Продемонстрированы все основные умения,. Решены все основные задачи. Выполнены все задания, в полном объеме без недочетов

Шкала оценки при промежуточной аттестации

Оценка	Уровень подготовки
зачтено	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
	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «отлично», при этом хотя бы одна компетенция сформирована на уровне «отлично»
	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «очень хорошо», при этом хотя бы одна компетенция сформирована на уровне « очень хорошо»
	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «хорошо», при этом хотя бы одна компетенция сформирована на уровне «хорошо»
	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «удовлетворительно», при этом хотя бы одна компетенция сформирована на уровне «удовлетворительно»
не зачтено	Хотя бы одна компетенция сформирована на уровне «неудовлетворительно», ни одна из компетенций не сформирована на уровне «плохо»
	Хотя бы одна компетенция сформирована на уровне «плохо»

5.2. Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения.

5.2.1. Контрольные вопросы

Вопросы	*Код формируемой компетенции*
1. Уязвимости. Классификация уязвимостей.	ПК-1

2. Понятие атак на компьютерные сети. Классификация атак на компьютерные сети. Основные типы сетевых атак.	ПК-1
3. Модель атаки. Результат атаки. Этапы реализации атак. Сокрытие источника и факта атаки.	ПК-1
4. Средства реализации атак.	ПК-1
5. Механизмы типовых атак, основанных на уязвимостях сетевых протоколов.	ПК-1
6. Атаки на сетевые службы. Атаки с использованием промежуточных узлов и территорий.	ПК-1
7. Технологии обнаружения компьютерных атак и их возможности.	ПК-1
8. Прямые и косвенные признаки атак. Источники информации об атаках	ПК-1
9. Методы обнаружения атак. Обнаружение аномалий и обнаружение злоупотреблений. Обнаружение следов атак.	ПК-1
10. Классификация систем обнаружения атак (СОА). Сетевые и узловые СОА.	ПК-1, ПК-10
11. Требования, предъявляемые к СОА.	ПК-1, ПК-10
12. Системы анализа защищенности. «Классические» системы обнаружения атак и анализаторы журналов регистрации. Обманные системы. Системы контроля целостности.	ПК-1
13. Определение политики и процедур безопасности.	ПК-1
14. Генерация информации для контроля целостности системных файлов данных.	ПК-1
15. Типовая архитектура СОА в составе сенсора, модуля управления, анализатора, набора протоколов взаимодействия и средства реагирования	ПК-10
16. Варианты размещения СОА.	ПК-10
17. Размещение сенсоров СОА.	ПК-10
18. Размещение системы анализа защищенности.	ПК-10
19. Размещение системы контроля целостности.	ПК-10
20. Размещение обманной системы.	ПК-10
21. Проблемы, связанные с СОА.	ПК-10
22. Реагирование на инциденты.	ПК-10
23. СОА Snort. Назначение, возможности.	ПК-10

5.2.2. Типовые задания для оценки сформированности компетенции ПК-1

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. Механизмы типовых атак, основанных на уязвимостях сетевых протоколов.
5. Атаки на сетевые службы. Атаки с использованием промежуточных узлов и территорий.
6. Технологии обнаружения компьютерных атак и их возможности.
7. Прямые и косвенные признаки атак. Источники информации об атаках.
8. Методы обнаружения атак. Обнаружение аномалий и обнаружение злоупотреблений. Обнаружение следов атак.
9. Классификация систем обнаружения атак (СОА). Сетевые и узловые СОА.
10. Требования, предъявляемые к СОА.

11. Системы анализа защищенности. «Классические» системы обнаружения атак и анализаторы журналов регистрации.
12. Обманные системы. Системы контроля целостности.
13. Определение политики и процедур безопасности.
14. Генерация информации для контроля целостности системных файлов и данных.

5.2.2. Типовые задания для оценки сформированности компетенции ПК-10

1. Классификация систем обнаружения атак (СОА). Сетевые и узловые СОА.
2. Требования, предъявляемые к СОА.
3. Типовая архитектура СОА в составе сенсора, модуля управления, анализатора, набора протоколов взаимодействия и средства реагирования.
4. Варианты размещения СОА.
5. Размещение сенсоров СОА.
6. Реагирование на инциденты.
7. СОА Snort. Назначение, возможности.
8. Механизмы типовых атак, основанных на уязвимостях сетевых протоколов.
9. Атаки на сетевые службы. Атаки с использованием промежуточных узлов и территорий.

6. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. «Стратегия национальной безопасности Российской Федерации до 2020 г.», утвержденная указом Президента Российской Федерации от 12.05.2009 № 537.
2. Лукацкий А.В. Обнаружение атак. 2003 г.

б) дополнительная литература:

1. SNORT Users Manual 2.9.9.

в) программное обеспечение и Интернет-ресурсы:

1. https://snort.org/

7. Материально-техническое обеспечение дисциплины

Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой, оснащенные оборудованием и техническими средствами обучения.

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 ОС ННГУ по направлению подготовки 02.04.02 «Фундаментальная информатика и информационные технологии».

Автор (ы) _____ Л.Ю. Ротков

_____ Р.Г. Нужный

Заведующий кафедрой «Безопасность информационных систем» _____ Л.Ю. Ротков

Программа одобрена на заседании методической комиссии радиофизического факультета от «25» мая 2023 года, протокол № 04/23.