

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
президиумом Ученого совета ННГУ
протокол от
«14» декабря 2021 г. № 4

Рабочая программа дисциплины

Системы обнаружения компьютерных атак
(наименование дисциплины (модуля))

Уровень высшего образования
специалитет
(бакалавриат / магистратура / специалитет)

Направление подготовки / специальность
10.05.02 Информационная безопасность телекоммуникационных систем
(указывается код и наименование направления подготовки / специальности)

Направленность образовательной программы
Системы подвижной цифровой защищенной связи
(указывается профиль / магистерская программа / специализация)

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

Нижний Новгород

2022

1. Место дисциплины в структуре ООП

Дисциплина «Системы обнаружения компьютерных атак» относится к дисциплинам части, формируемой участниками образовательных отношений, основной образовательной программы по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем».

№ 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.05.02 «Системы обнаружения компьютерных атак» относится к части ООП специальности 10.05.02 «Информационная безопасность телекоммуникационных систем», 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-2. Способен анализировать угрозы информационной безопасности цифровых телекоммуникационных сетей, контролировать их работоспособность и оценивать эффективность	ПК-2.1. Знает: - методы создания моделей угроз информационной безопасности цифровых телекоммуникационных сетей - способы оценки уязвимостей цифровых телекоммуникационных сетей с точки зрения возможности НСД к ним	Знать: - модели угроз информационной безопасности цифровых телекоммуникационных сетей - методики оценки уязвимостей цифровых телекоммуникационных сетей с точки зрения возможности НСД	Собеседование
	ПК-2.2. Умеет: - разрабатывать модели угроз и систематизировать сведения об угрозах информационной безопасности	Уметь: - анализировать модели угроз и систематизировать сведения об угрозах информационной безопасности	Собеседование
	ПК-2.3. Владеет: - навыками сбора и	Владеть: - навыками обработки сведений об	Собеседование

	систематизации сведений об угрозах НСД к системам подвижной цифровой защищенной связи	угрозах НСД к системам подвижной цифровой защищенной связи	
ПК-4. Способен проводить научные исследования принципов позиционирования подвижных объектов и реализовывать их в системах подвижной цифровой защищенной связи	ПК-4.1. Знает: - национальные, межгосударственные и международные стандарты, устанавливающие требования по защите информации, анализу защищенности систем позиционирования подвижных объектов и - методы, способы, средства, последовательность и содержание этапов разработки средств защиты систем позиционирования подвижных объектов	Знать: - национальные, межгосударственные и международные стандарты, устанавливающие требования по защите информации, анализу защищенности систем позиционирования подвижных объектов - методики оценки последствий нарушения информационной безопасности защищенности систем позиционирования подвижных объектов - методики выполнения этапов разработки средств защиты систем позиционирования подвижных объектов	Собеседование
	ПК-4.2. Умеет: - проводить сбор и анализ исходных данных для разработки средств и систем защиты и обеспечивать рациональный выбор элементной базы систем подвижной цифровой защищенной связи	Уметь: - обрабатывать данные в процессе разработки средств и систем защиты и обеспечивать рациональный выбор элементной базы систем подвижной цифровой защищенной связи	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, форма промежуточной аттестации по дисциплине	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	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.

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				
<u>Знания</u>	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, без ошибок.	Уровень знаний в объеме, превышающем программу подготовки.
<u>Умения</u>	Отсутствие минимальных умений . Невозможность оценить наличие умений вследствие отказа обучающегося от ответа	При решении стандартных задач не продемонстрированы основные умения. Имели место грубые ошибки.	Продemonстрированы основные умения. Решены типовые задачи с негрубыми ошибками. Выполнены все задания, но не в полном объеме.	Продemonстрированы все основные умения. Решены все основные задачи с негрубыми ошибками. Выполнены все задания, в полном объеме, но некоторые с недочетами.	Продemonстрированы все основные умения. Решены все основные задачи . Выполнены все задания, в полном объеме, но некоторые с недочетами.	Продemonстрированы все основные умения, решены все основные задачи с отдельными несущественными недочетами, выполнены все задания в полном объеме.	Продemonстрированы все основные умения, . Решены все основные задачи. Выполнены все задания, в полном объеме без недочетов
<u>Навыки</u>	Отсутствие владения материалом. 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	Продemonстрированы базовые навыки при решении стандартных задач с некоторыми недочетами	Продemonстрированы базовые навыки при решении стандартных задач без недочетов.	Продemonстрированы навыки при решении нестандартных задач без ошибок и недочетов.	Продemonстрирован творческий подход к решению нестандартных задач

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-2
2. Понятие атак на компьютерные сети. Классификация атак на компьютерные сети. Основные типы сетевых атак.	ПК-2
3. Модель атаки. Результат атаки. Этапы реализации атак. Соккрытие источника и факта атаки.	ПК-2
4. Средства реализации атак.	ПК-2
5. Механизмы типовых атак, основанных на уязвимостях сетевых протоколов.	ПК-2, ПК-4
6. Атаки на сетевые службы. Атаки с использованием промежуточных узлов и территорий.	ПК-2, ПК-4
7. Технологии обнаружения компьютерных атак и их возможности.	ПК-2
8. Прямые и косвенные признаки атак. Источники информации об атаках	ПК-2
9. Методы обнаружения атак. Обнаружение аномалий и обнаружение злоупотреблений. Обнаружение следов атак.	ПК-2
10. Классификация систем обнаружения атак (СОА). Сетевые и узловые СОА.	ПК-2
11. Требования, предъявляемые к СОА.	ПК-2
12. Системы анализа защищенности. «Классические» системы обнаружения атак и анализаторы журналов регистрации. Обманные	ПК-2

системы. Системы контроля целостности.	
13. Определение политики и процедур безопасности.	ПК-2, ПК-4
14. Генерация информации для контроля целостности системных файлов данных.	ПК-2
15. Типовая архитектура СОА в составе сенсора, модуля управления, анализатора, набора протоколов взаимодействия и средства реагирования.	ПК-2
16. Варианты размещения СОА.	ПК-2
17. Размещение сенсоров СОА.	ПК-2
18. Размещение системы анализа защищенности.	ПК-2
19. Размещение системы контроля целостности.	ПК-2
20. Размещение обманной системы.	ПК-2
21. Проблемы, связанные с СОА.	ПК-2
22. Реагирование на инциденты.	ПК-2
23. СОА Snort. Назначение, возможности.	ПК-2

5.2.2. Типовые задания для оценки сформированности компетенции ПК-2

1. Понятие атак на компьютерные сети. Классификация атак на компьютерные сети. Основные типы сетевых атак.
2. Модель атаки. Результат атаки. Этапы реализации атак. Скрытие 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.

5.2.3. Типовые задания для оценки сформированности компетенции ПК-4

1. Механизмы типовых атак, основанных на уязвимостях сетевых протоколов.
2. Атаки на сетевые службы. Атаки с использованием промежуточных узлов и территорий.
3. Определение политики и процедур безопасности.

6. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. «Стратегия национальной безопасности Российской Федерации до 2020г», 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 ФГОС ВО по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем».

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 «09» декабря 2021 года, протокол № 07/21.