

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**

Системы обнаружения компьютерных атак

---

Уровень высшего образования

Магистратура

---

Направление подготовки / специальность

02.04.02 - Фундаментальная информатика и информационные технологии

---

Направленность образовательной программы

Информационная безопасность и защита информации

---

Форма обучения

очная

---

г. Нижний Новгород

2024 год начала подготовки

## 1. Место дисциплины в структуре ОПОП

Дисциплина Б1.В.ДВ.04.01 Системы обнаружения компьютерных атак относится к части, формируемой участниками образовательных отношений 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
ПК-1: Способен руководить научными исследованиями и опытно-конструкторскими разработками, в области информатики и информационных технологий (ФИИТ), и формировать их новые направления в области профессиональной деятельности	<p>ПК-1.1: Знает проблематику и методы научных исследований и опытно-конструкторских разработок в области ФИИТ применительно к профессиональной деятельности</p> <p>ПК-1.2: Имеет навыки выполнения научных исследований и опытно-конструкторских разработок в области ФИИТ применительно к профессиональной деятельности</p> <p>ПК-1.3: Имеет навыки руководства исследованиями и опытно-конструкторскими разработками в области ФИИТ применительно к профессиональной деятельности, и формирования их новых направлений</p>	<p>ПК-1.1: Знать: - проблематику и методы научных исследований и опытно-конструкторских разработок в области построения систем обнаружения компьютерных атак</p> <p>ПК-1.2: Уметь: - выполнять научные исследования и опытно-конструкторские разработки в области построения систем обнаружения компьютерных атак</p> <p>ПК-1.3: Владеть: - навыками руководства исследованиями и опытно-конструкторскими разработками в области построения систем обнаружения компьютерных атак</p>	Собеседование	Зачёт: Контрольные вопросы
ПК-10: Способен применять в профессиональной деятельности стандарты, процедуры и средства	ПК-10.1: Знает стандарты, процедуры и средства администрирования и управления безопасностью информационных технологий	ПК-10.1: Знать: - стандарты, процедуры и средства администрирования и управления безопасностью информационных технологий в	Собеседование	Зачёт: Контрольные вопросы

администрирования и управления безопасностью информационных технологий; способен использовать стандарты, процессы, процедуры и средства поддержки жизненного цикла информационных технологий	<p>ПК-10.2: Умеет применять в профессиональной деятельности стандарты, процедуры и средства администрирования и управления безопасностью информационных технологий</p> <p>ПК-10.3: Имеет практический опыт использования стандартов, процессов, процедур и средств поддержки жизненного цикла информационных технологий</p>	<p>области построения систем обнаружения компьютерных атак</p> <p>ПК-10.2: Уметь: - применять в профессиональной деятельности стандарты, процедуры и средства администрирования и управления безопасностью информационных технологий в области построения систем обнаружения компьютерных атак</p> <p>ПК-10.3: Владеть: - опытом использования стандартов, процессов, процедур и средств поддержки жизненного цикла информационных технологий в области построения систем обнаружения компьютерных атак</p>		
--	---	---	--	--

### 3. Структура и содержание дисциплины

#### 3.1 Трудоемкость дисциплины

	<b>очная</b>
<b>Общая трудоемкость, з.е.</b>	<b>3</b>
<b>Часов по учебному плану</b>	<b>108</b>
в том числе	
<b>аудиторные занятия (контактная работа):</b>	
- занятия лекционного типа	32
- занятия семинарского типа (практические занятия / лабораторные работы)	0
- КСР	1
<b>самостоятельная работа</b>	<b>75</b>
<b>Промежуточная аттестация</b>	<b>0</b>
	<b>Зачёт</b>

#### 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/ лабора торные работы), часы	Всего	
	0 Ф 0	0 Ф 0	0 Ф 0	0 Ф 0	0 Ф 0
1. Нормативная база в области информационной безопасности	28	6		6	22
2. Системы обнаружения компьютерных атак	79	26		26	53
Аттестация	0				
КСР	1			1	
Итого	108	32	0	33	75

### Содержание разделов и тем дисциплины

1. Нормативная база в области информационной безопасности
2. Системы обнаружения компьютерных атак

Практические занятия /лабораторные работы организуются, в том числе, в форме практической подготовки, которая предусматривает участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

На проведение практических занятий / лабораторных работ в форме практической подготовки отводится: очная форма обучения - 8 ч.

#### 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 ПК-1:

1. Уязвимости. Классификация уязвимостей.

2. Механизмы типовых атак, основанных на уязвимостях сетевых протоколов.
3. Технологии обнаружения компьютерных атак и их возможности.
4. Прямые и косвенные признаки атак. Источники информации об атаках.
5. Методы обнаружения атак. Обнаружение аномалий и обнаружение злоупотреблений. Обнаружение следов атак.

### 5.1.2 Типовые задания (оценочное средство - Собеседование) для оценки сформированности компетенции ПК-10:

1. Классификация систем обнаружения атак (СОА). Сетевые и узловые СОА.
2. Системы анализа защищенности. «Классические» системы обнаружения атак и анализаторы журналов регистрации. Обманные системы. Системы контроля целостности.
3. Генерация информации для контроля целостности системных файлов и данных.
4. Размещение системы анализа защищенности.
5. Размещение системы контроля целостности.
6. Размещение обманной системы.
7. Проблемы, связанные с СОА.

### 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 (индикатор достижения компет	плохо	неудовлетворительно	удовлетворительно	хорошо	очень хорошо	отлично	превосходно
	не зачтено		зачтено				

компетенций)							
<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. Ошибок нет.	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 и 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 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 некоторым и недочетами	Продemonстрированы базовые навыки при решении стандартных задач с некоторым и недочетами	Продemonстрированы базовые навыки при решении стандартных задач без ошибок и недочетов	Продemonстрированы навыки при решении нестандартных задач без ошибок и недочетов	Продemonстрирован 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».
	удовлетворительно	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»
<b>не зачтено</b>	<b>неудовлетворительно</b>	Хотя бы одна компетенция сформирована на уровне «неудовлетворительно».
	<b>плохо</b>	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 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. 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.

#### **5.3.2 Типовые задания (оценочное средство - Контрольные вопросы) для оценки сформированности компетенции ПК-10**

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.

#### **Критерии оценивания (оценочное средство - Контрольные вопросы)**

Оценка	Критерии оценивания
зачтено	Все компетенции (части компетенций), на формирование которых направлена дисциплина,

Оценка	Критерии оценивания
	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. Технологии защиты информации в компьютерных сетях / Руденков Н.А., Пролетарский А.В., Смирнова Е.В., Суоров А.М. - Москва : ИНТУИТ, 2016., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=663523&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>.

Дополнительная литература:

1. Без автора. Стратегия национальной безопасности Российской Федерации : Нормативные документы. - 3. - Москва : ООО "Научно-издательский центр ИНФРА-М", 2024. - 101 с. - Дополнительное профессиональное образование. - ISBN 978-5-16-016495-3. - ISBN 978-5-16-108765-7., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=889830&idb=0>.
2. Внуков А. А. Защита информации : учебное пособие / А. А. Внуков. - 3-е изд. ; пер. и доп. - Москва : Юрайт, 2023. - 161 с. - (Высшее образование). - ISBN 978-5-534-07248-8. - Текст : электронный // ЭБС "Юрайт"., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=839576&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.

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/специальности 02.04.02 - Фундаментальная информатика и информационные технологии.

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.