

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

Спецлаборатории

(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 год

1. Место дисциплины в структуре ООП

Дисциплина «Спецлаборатории» 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.05 «Спецлаборатории» 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 безопасности информационных технологий	Собеседование
	ПК-1.2. Умеет выполнять научные исследования и опытно-конструкторские разработки в области ФИИТ применительно к профессиональной деятельности	Уметь: - проводить научные исследования и опытно-конструкторские разработки в области безопасности информационных технологий	Собеседование
	ПК-1.3. Имеет навыки руководства исследованиями и опытно-конструкторскими разработками в области ФИИТ	Владеть: - навыками руководства исследованиями и опытно-конструкторскими разработками в области безопасности информационных технологий	Собеседование

	применительно к профессиональной деятельности, и формирования их новых направлений		
ПК-5. Способен демонстрировать общенаучные базовые знания математических и естественных наук, фундаментальной информатики и информационных технологий; способен применять в профессиональной деятельности современные языки программирования и методы параллельной обработки данных, операционные системы, электронные библиотеки и пакеты программ, сетевые технологии	ПК-5.1. Знает основы научно-исследовательской деятельности в области информационных технологий, владеет знанием основ философии и методологии науки; знанием методов научных исследований и навыками их проведения.	Знать: - методы проведения научных исследований - пакеты прикладных программ исследования сетевых технологий	Собеседование
	ПК-5.2. Умеет применять полученные знания в области фундаментальных научных основ теории информации и решать стандартные задачи в собственной научно-исследовательской деятельности.	Уметь: - применять в профессиональной деятельности операционные системы - применять в профессиональной деятельности электронные библиотеки - применять в профессиональной деятельности пакеты программ - применять в профессиональной деятельности сетевые технологии	Задачи (практические задания)
	ПК-5.3. Имеет практический опыт научно-исследовательской деятельности в области информационных технологий.	Владеть: - практическим опытом научно-исследовательской деятельности в области информационных технологий	Задачи (практические задания)

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. Система обнаружения вторжений Snort	33			16	16	37
2. Организация юридически значимого электронного документооборота с использованием электронной подписи	36			16	16	38
Итого:	107			32	32	75

4. Учебно-методическое обеспечение самостоятельной работы обучающихся

Самостоятельная работа обучающихся включает в себя изучение дополнительных разделов методических описаний лабораторных работ.

Текущий контроль успеваемости реализуется в рамках занятий лабораторного типа, групповых и индивидуальных консультаций.

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						
	плохо	неудовлетворительно	удовлетворительно	хорошо	очень хорошо	отлично	превосходно
	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 незначительных 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 незначительными 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
	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
зачтено	отлично	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»
	очень хорошо	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»
	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»
	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»
не зачтено	неудовлетворительно	Хотя бы одна компетенция сформирована на уровне «неудовлетворительно», ни одна из компетенций не сформирована на уровне «плохо»
	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

<i>Вопросы</i>	<i>Код формируемой компетенции</i>
1. Уязвимости. Классификация уязвимостей.	ПК-1, ПК-5
2. Понятие атак на компьютерные сети. Классификация атак на компьютерные сети. Основные типы сетевых атак.	ПК-1, ПК-5
3. Модель атаки. Результат атаки. Этапы реализации атак. Скрытие источника и факта атаки.	ПК-1, ПК-5
4. Средства реализации атак.	ПК-1, ПК-5
5. Механизмы типовых атак, основанных на уязвимостях сетевых протоколов.	ПК-1, ПК-5
6. Атаки на сетевые службы. Атаки с использованием промежуточных узлов и территорий.	ПК-1, ПК-5
7. Технологии обнаружения компьютерных атак и их возможности.	ПК-1, ПК-5
8. Прямые и косвенные признаки атак. Источники информации об атаках	ПК-1, ПК-5
9. Методы обнаружения атак. Обнаружение аномалий и обнаружение злоупотреблений. Обнаружение следов атак.	ПК-1, ПК-5
10. Классификация систем обнаружения атак (СОА). Сетевые и узловые СОА.	ПК-1, ПК-5
11. Требования, предъявляемые к СОА.	ПК-1, ПК-5
12. Системы анализа защищенности. «Классические» системы обнаружения атак и анализаторы журналов регистрации. Обманные системы. Системы контроля целостности.	ПК-1, ПК-5
13. Определение политики и процедур безопасности.	ПК-1, ПК-5
14. Генерация информации для контроля целостности системных файлов данных.	ПК-1, ПК-5
15. Типовая архитектура СОА в составе сенсора, модуля управления, анализатора, набора протоколов взаимодействия и средства реагирования	ПК-1, ПК-5
16. Варианты размещения СОА.	ПК-1, ПК-5
17. Размещение сенсоров СОА.	ПК-1, ПК-5
18. Размещение системы анализа защищенности.	ПК-1, ПК-5
19. Размещение системы контроля целостности.	ПК-1, ПК-5
20. Размещение обманной системы.	ПК-1, ПК-5
21. Проблемы, связанные с СОА.	ПК-1, ПК-5
22. Реагирование на инциденты.	ПК-1, ПК-5
23. СОА Snort. Назначение, возможности.	ПК-1, ПК-5
24. Сервисы безопасности Рекомендаций X.800.	ПК-1, ПК-5
25. Некриптографические механизмы безопасности.	ПК-1, ПК-5
26. Криптографические механизмы безопасности.	ПК-1, ПК-5
27. Основные системы, в которых применяется PKI.	ПК-1, ПК-5
28. Основные компоненты PKI.	ПК-1, ПК-5
29. Сервисы PKI.	ПК-1, ПК-5
30. Архитектуры PKI. Взаимодействие компонентов PKI.	ПК-1, ПК-5

31. Функции PKI.	ПК-1, ПК-5
32. Жизненный цикл сертификата.	ПК-1, ПК-5
33. Классификация шифров.	ПК-1, ПК-5
34. Нарисуйте схему PKI, ее линии взаимодействия.	ПК-1, ПК-5
35. Определите, в какие хранилища были установлены сертификаты.	ПК-1, ПК-5
36. Определите дату выпуска последнего списка отозванных сертификатов УЦ и дату следующего выпуска.	ПК-1, ПК-5
37. Нарисуйте схему движения писем электронной почты с пояснениями по стадиям. На этапах использования ЭП и шифрования поясните применение открытых, закрытых ключей и сертификатов открытых ключей.	ПК-1, ПК-5
38. Перечислите основные отечественные стандарты в области криптографии?	ПК-1, ПК-5
39. Каким образом можно обеспечить поддержку отечественных криптографических алгоритмов в ОС.	ПК-1, ПК-5
40. По каким причинам в работе используется СКЗИ в режиме КС1?	ПК-1, ПК-5
41. В чем принципиальное отличие классов КС1 и КС2?	ПК-1, ПК-5
42. Какие датчики случайных чисел (ДСЧ) и носители ключевого материала использовались в работе?	ПК-1, ПК-5

5.2.2. Типовые задания для оценки сформированности компетенций ПК-1, ПК-5

Задание 1.

Посмотреть наличие/отсутствие зафиксированных событий безопасности. В случае наличия событий безопасности объяснить причину.

Задание 2.

Посмотреть наличие/отсутствие зафиксированных событий безопасности. Указать:

- общее количество зафиксированных событий безопасности;
- количество зафиксированных уникальных событий безопасности.

Для каждого из уникальных событий указать:

- общее количество;
- количество уникальных адресов источника и назначения;
- время первого и последнего события безопасности;
- на использование какой уязвимости направлена зафиксированная попытка вторжения.

Задание 3.

Создать в соответствии с заданием правило для COB Snort. Добавить созданное правило в сигнатуры COB Snort.

Задание 4.

Настройка Центра сертификации на машине;
Установка и настройка СКЗИ КриптоПро CSP;
Установка необходимых компонентов операционной системы;

Задание 5.

Издание и установка сертификата серверной аутентификации WEB-сервера ЦС;
Установка Центра Сертификации КриптоПро;
Создание и настройка Центра регистрации на машине;

Задание 6.

Издание и установка сертификата серверной аутентификации WEB-сервера ЦР;
Выпуск и установка клиентского сертификата ЦР;
Настройка соединения Центра Регистрации с Центром Сертификации;
Создание АРМ администратора на машине.

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.
3. Федеральный закон Российской Федерации от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи».
4. Федеральный закон Российской Федерации от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
5. Приказ ФАПСИ от 13 июня 2001 года № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».
6. Балыбердин А.В., Корелов СВ., Рябов А.А. Организация юридически значимого электронного документооборота с использованием электронной подписи: Учебно-методическое пособие. - Нижний Новгород: Нижегородский госуниверситет, 2013. - 44 с.

б) дополнительная литература:

1. SNORT Users Manual 2.9.9.
2. Алферов А.П. Основы криптографии: учеб. пособие. - М: Гелиос АРВ, 2001.
3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С. - М: Триумф, 2003.

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

_____ А.А. Горбунов

Заведующий кафедрой «Безопасность
информационных систем» _____

_____ Л.Ю. Ротков

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