

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

Технологии анализа безопасности мобильных систем
(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)

Нижегород

2022 год

1. Место дисциплины в структуре ООП

Дисциплина «Технологии анализа безопасности мобильных систем» относится к дисциплинам обязательной части 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
1	Блок 1. Дисциплины (модули) Обязательная часть	Дисциплина Б1.О.41 «Технологии анализа безопасности мобильных систем» относится к обязательной части ООП специальности 10.05.02 «Информационная безопасность телекоммуникационных систем»

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	
ОПК-11.2 Способен контролировать работоспособность и оценивать эффективность средств защиты информации в системах подвижной цифровой защищенной связи	ОПК-11.2.1. Знает: - методы контроля работоспособности и оценки эффективности средств защиты информации в системах подвижной цифровой защищенной связи	Знать: - общие свойства и взаимозависимости различных видов моделей программных объектов - методы контроля работоспособности и оценки эффективности средств защиты информации в системах подвижной цифровой защищенной связи	Собеседование
	ОПК-11.2.2. Умеет: - оценивать эффективность средств защиты информации в системах подвижной цифровой защищенной связи	Уметь: - определять параметры программно-аппаратных систем - оценивать и анализировать основные характеристики функциональных частей операционных систем - оценивать эффективность средств защиты информации в системах подвижной цифровой защищенной связи	Собеседование
	ОПК-11.2.3. Владеет: - навыками контроля работоспособности средств защиты информации в системах подвижной цифровой защищенной связи	Владеть: - навыками контроля работоспособности средств защиты информации в системах 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	4 ЗЕТ	___ ЗЕТ	___ ЗЕТ
Часов по учебному плану	144		
в том числе			
аудиторные занятия (контактная работа): - занятия лекционного типа - занятия семинарского типа (практические занятия / лабораторные работы)	64		
самостоятельная работа	33		
КСР	2		
Промежуточная аттестация – экзамен/зачет	экзамен 45		

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. Состав системы SIEM: система управления информационной безопасностью (SIM), система управления событиями безопасности (SEM)	8		2	2	4	4
2. Задачи, решаемые	8		2	2	4	4

SIEM-системой: сбор, обработка и анализ событий безопасности, обнаружение атак и нарушений критериев и политик безопасности, оперативная оценка защищенности ресурсов, анализ и управление рисками безопасности, проведение расследований инцидентов, принятие решений по защите информации, формирование отчетных документов						
3. Источники данных для SIEM-систем: Access Control, Authentication, DLP-системы, IDS/IPS-системы, антивирусные приложения, журналы событий серверов и рабочих станций, межсетевые экраны, сетевое активное оборудование, сканеры уязвимостей, системы инвентаризации и asset-management, системы веб-фильтрации	10		3	3	6	4
4. Архитектура SIEM-системы. Уровни построения SIEM-системы: сбор данных, управление данными, анализ данных	28		11	11	22	6
5. Функционирование SIEM	33		11	11	22	11
6. Обзор современных систем: Tivoli Security Information and Event Manager (TSIEM), Splunk, LogRhythm, Inc. Отечественные решения SIEM: KOMRAD Enterprise SIEM, Security Capsule, MaxPatrol SIEM,	10		3	3	6	4

RUSIEM						
Итого:	97		32	32	64	33

4. Учебно-методическое обеспечение самостоятельной работы обучающихся

Самостоятельная работа обучающихся включает следующие виды:

- изучение дополнительных разделов дисциплины с использованием учебной литературы.

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	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	Продemonстрированы все основные умения,. Решены все основные задачи. Выполнены все задания, в полном объеме без недочетов

				недочетами.		объеме.	
<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	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 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. Что такое система управления информационной безопасностью	ОПК-11.2
2. Что такое система управления событиями безопасности	ОПК-11.2
3. Какие задачи, решает SIEM-система	ОПК-11.2
4. Какие источники данных в SIEM-системе	ОПК-11.2
5. Какая архитектура SIEM-системы	ОПК-11.2
6. Этапы функционирования SIEM-системы	ОПК-11.2

6. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Герасименко В.А. Защита информации в АСОД.- М.: Энергоиздат, 1994.
2. Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации. Под. ред. А.С.Маркова. -М.:Радио и связь, 2012. 192 с.
3. Сидак А.А., Ильин А.В., Кубарев А.В. Мобильные устройства в информационных системах и угрозы безопасности информации. Взаимосвязи. // Вопросы кибербезопасности. №4.2014.
4. Васильев, В. И. Интеллектуальные системы защиты информации: Учебное пособие. – М.: Машиностроение, 2013. – 82 с.
5. Гузаиров, М. Б., Машкина, И. В. Управление защитой информации на основе интеллектуальных технологий: учебное пособие. – М.: Машиностроение, 2013. – 241 с.

б) дополнительная литература:

1. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. - М.: Гостехкомиссия России, 1998.
2. ГОСТ Р ИСО/МЭК 15408-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Части 1, 2, 3. - М.: ИПК «Изд-во стандартов», 2002.
3. ГОСТ РВ 51719-2001. Испытания программной продукции. - М.: ИПК «Изд-во стандартов», 2001.
4. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Части 1, 2, 3. - М.: Гостехкомиссия России, 2002
5. <http://msdn.microsoft.com/library/en-us/dnpag2/html/SecurityDeploymentReviewIndex.asp>.

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

_____ А.А. Горбунов

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

Программа одобрена на заседании методической комиссии радиофизического факультета от «09» **декабря** 2021 года, протокол № 07/21.