

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

Технологии анализа безопасности мобильных систем

Уровень высшего образования

Специалитет

Направление подготовки / специальность

10.05.02 - Информационная безопасность телекоммуникационных систем

Направленность образовательной программы

Системы подвижной цифровой защищенной связи

Форма обучения

очная

г. Нижний Новгород

2024 год начала подготовки

1. Место дисциплины в структуре ОПОП

Дисциплина Б1.О.41 Технологии анализа безопасности мобильных систем относится к обязательной части 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
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 ОПК-11.2..2: Умеет: - оценивать эффективность средств защиты информации в системах подвижной цифровой защищенной связи ОПК-11.2..3: Владеет: - навыками контроля работоспособности средств защиты информации в системах подвижной цифровой защищенной связи	ОПК-11.2..1: 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 ОПК-11.2..2: 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 ОПК-11.2..3: Владеть: - навыками контроля работоспособности средств защиты информации в системах подвижной цифровой защищенной связи	Собеседование	Экзамен: Контрольные вопросы

3. Структура и содержание дисциплины

3.1 Трудоемкость дисциплины

	очная
Общая трудоемкость, з.е.	4
Часов по учебному плану	144
в том числе	
аудиторные занятия (контактная работа):	
- занятия лекционного типа	0
- занятия семинарского типа (практические занятия / лабораторные работы)	64
- КСР	2
самостоятельная работа	33
Промежуточная аттестация	45 Экзамен

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. Состав системы SIEM: система управления информационной безопасностью (SIM), система управления событиями безопасности (SEM)	8		4	4	4
2. Задачи, решаемые 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	8		4	4	4
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		6	6	4
4. Архитектура SIEM-системы. Уровни построения SIEM-системы: сбор данных, управление данными, анализ данных	28		22	22	6
5. Функционирование SIEM	33		22	22	11
6. Обзор современных систем: Tivoli Security Information and Event Manager (TSIEM), Splunk, LogRhythm, Inc. Отечественные решения	10		6	6	4

SIEM: KOMRAD Enterprise SIEM, Security Capsule, MaxPatrol SIEM, RUSIEM					
Аттестация	45				
КСР	2			2	
Итого	144	0	64	66	33

Содержание разделов и тем дисциплины

1. Состав системы SIEM: система управления информационной безопасностью (SIM), система управления событиями безопасности (SEM)
2. Задачи, решаемые 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
4. Архитектура SIEM-системы. Уровни построения SIEM-системы: сбор данных, управление данными, анализ данных
5. Функционирование SIEM
6. Обзор современных систем: Tivoli Security Information and Event Manager (TSIEM), Splunk, LogRhythm, Inc. Отечественные решения SIEM: KOMRAD Enterprise SIEM, Security Capsule, MaxPatrol SIEM, RUSIEM

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 - 4 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 ОПК-11.2.:

1. Нарисуйте схему архитектура SIEM-системы.
2. Определите источники данных для SIEM-системы в DLP.
3. Определите источники данных для SIEM-системы в системе аутентификации.
4. Определите источники данных для SIEM-системы в системе управления доступом.
5. Определите источники данных для SIEM-системы в журналах событий.

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 (индикатора достижения 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 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	Продемонстрированы основные умения. Решены типовые задачи с негрубыми ошибками. Выполнены все задания, но	Продемонстрированы все основные умения. Решены все основные задачи с негрубыми ошибками. Выполнены все задания	Продемонстрированы все основные умения. Решены все основные задачи. Выполнены все задания в полном объеме, но	Продемонстрированы все основные умения. Решены все основные задачи с отдельным и несущест	Продемонстрированы все основные умения. Решены все основные задачи. Выполнены все задания, в полном объеме без недочетов

			не в полном объеме	в полном объеме, но некоторые с недочетами	некоторые с недочетами	енными недочетам и, выполнены все задания в полном объеме	
<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	Продемонстрированы базовые навыки при решении стандартных задач с некоторым и 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 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»
не зачтено	неудовлетворительно	Хотя бы одна компетенция сформирована на уровне «неудовлетворительно».
	плохо	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 ОПК-11.2.

1. Что такое система управления информационной безопасностью
2. Что такое система управления событиями безопасности
3. Какие задачи, решает SIEM-система

4. Какие источники данных в SIEM-системе
5. Какая архитектура SIEM-системы
6. Этапы функционирования SIEM-системы

Критерии оценивания (оценочное средство - Контрольные вопросы)

Оценка	Критерии оценивания
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»
неудовлетворительно	Хотя бы одна компетенция сформирована на уровне «неудовлетворительно»
плохо	Хотя бы одна компетенция сформирована на уровне «плохо»

6. Учебно-методическое и информационное обеспечение дисциплины (модуля)

Основная литература:

1. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения / Белоус А.И., Солодуха В.А. - Москва : Техносфера, 2021., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=789929&idb=0>.
2. Васильев В.И. Интеллектуальные системы защиты информации : учебное пособие / Васильев В.И. - Москва : Машиностроение, 2021. - 172 с. - ISBN 978-5-907104-99-0., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=808491&idb=0>.
3. Казарин О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум / О. В. Казарин, А. С. Забабурин. - Москва : Юрайт, 2023. - 312 с. - (Высшее образование). - ISBN 978-5-9916-9043-0. - Текст : электронный // ЭБС "Юрайт"., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=846565&idb=0>.

Дополнительная литература:

1. Сертификация программного обеспечения. Статический анализ программного кода : учебно-методическое пособие / Антонова В.М.; Астрахов А.В.; Кондаков С.Е.; Куликов Л.С.; Щербаков А.В. - Москва : МГТУ им. Н.Э. Баумана, 2019. - 22 с. - ISBN 978-5-7038-5043-5., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=773451&idb=0>.
2. Иванько А. Ф. Системное программное обеспечение информационных мультимедиа-систем / Иванько А. Ф., Иванько М. А. - Санкт-Петербург : Лань, 2020. - 80 с. - Библиогр.: доступна в карточке книги, на сайте ЭБС Лань. - Книга из коллекции Лань - Информатика. - ISBN 978-5-8114-4927-9., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=708259&idb=0>.
3. Казарин О. В. Надежность и безопасность программного обеспечения : учебное пособие / О. В. Казарин, И. Б. Шубинский. - Москва : Юрайт, 2023. - 342 с. - (Высшее образование). - ISBN 978-5-534-05142-1. - Текст : электронный // ЭБС "Юрайт"., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=842944&idb=0>.
4. Сеницын И. В. Встраиваемые системы управления базами данными для мобильных приложений : учебное пособие / Сеницын И. В., Воронцов Ю. А., Михайлова Е. К. - Москва : РТУ МИРЭА, 2022. - 529 с. - Книга из коллекции РТУ МИРЭА - Информатика., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=828348&idb=0>.
5. Полтавцева Мария Анатольевна. Высокопроизводительные системы обнаружения вторжений : Учебное пособие; Учебное пособие / Санкт-Петербургский государственный политехнический университет Петра Великого. - 2. - Вологда : Инфра-Инженерия, 2023. - 152 с. - ВО - Бакалавриат. - ISBN 978-5-9729-1213-1., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=876071&idb=0>.

Программное обеспечение и Интернет-ресурсы (в соответствии с содержанием дисциплины):

1. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Части 1, 2, 3. - М.: Гостехкомиссия России, 2002. (<https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rukovodyashchij-dokument-ot-19-iyunya-2002-g-n-187>)
2. 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, 1999. (<https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rukovodyashchij-dokument-ot-4-iyunya-1999-g-n-114>)
3. ГОСТ Р ИСО/МЭК 15408-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Части 1, 2, 3. - М.: ИПК Издательство стандартов, 2002. (<https://docs.cntd.ru/document/1200029952>)

7. Материально-техническое обеспечение дисциплины (модуля)

Учебные аудитории для проведения учебных занятий, предусмотренных образовательной программой, оснащены мультимедийным оборудованием (проектор, экран), техническими средствами обучения, компьютерами.

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 направлению подготовки/специальности 10.05.02 - Информационная безопасность телекоммуникационных систем.

Автор(ы): Ротков Леонид Юрьевич, кандидат технических наук, доцент
Горбунов Александр Александрович.

Заведующий кафедрой: Ротков Леонид Юрьевич, кандидат технических наук.

Программа одобрена на заседании методической комиссии от 18 декабря 2023 года, протокол № 09/23.