МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Самарский государственный технический университет»
(ФГБОУ ВО «СамГТУ»)

УТВЕРЖДАЮ:
Проректор по учебной работе

_____
(подпись, ФИО)
«____»_____20__ г.

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

Методология и организация информационно-аналитического мониторинга

УГСН	10.00.00 Информационная безопасность
Направление подготовки (специальность)	10.03.01 Информационная безопасность
Квалификация	*Бакалавр*
Форма обучения	*Очная*
Год начала подготовки	*2023*
Объем дисциплины, ч. / з.е. / недели	*108/3/2*
Образовательные технологии	*Традиционные*
Форма контроля (промежуточная аттестация)	*Семестр 1: Зачет*
Подразделение – разработчик	*Кафедра "Электронные системы и информационная безопасность"*

Самара 2023

Разработчик

Разработчик РПМ
Карпова Надежда Евгеньевна
Руководитель подразделения
-

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по модулю, соотнесенных с планируемыми результатами освоения образовательной программы 3

2. Место модуля в структуре образовательной программы 3

3. Объем модуля в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся 4

4. Содержание модуля, структурированное по темам (разделам), с указанием отведенного на них количества академических часов и видов учебных занятий 5

4.1. Содержание лекционных занятий 6

4.2. Содержание лабораторных занятия 7

4.3. Содержание практических занятий 8

4.4. Содержание самостоятельной работы 9

5. Перечень учебной литературы и учебно-методического обеспечения по модулю 9

6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», профессиональных баз данных, информационно-справочных систем 10

7. Описание материально-технической базы, необходимой для осуществления образовательного процесса по модулю 10

ПРИЛОЖЕНИЕ 11

Фонд оценочных средств 11

1. Перечень планируемых результатов обучения по модулю, соотнесенных с планируемыми результатами освоения образовательной программы

Таблица 1

Наименование категории (группы) компетенций	**Код и наименование компетенции**	**Код и наименование индикатора достижения компетенции**	**Результаты обучения** (знать, уметь, владеть)
Профессиональные компетенции			
-	ПК-4 Способен обеспечить информационную безопасность объектов информатизации в процессе их эксплуатации	ПК-4.1 Знает принципы работы и правила эксплуатации объектов информатизации, подлежащих защите	Знать принципы работы и правила эксплуатации объектов информатизации, подлежащих защите
		ПК-4.2 Умеет обеспечивать информационную безопасность объектов информатизации в соответствии с правилами их эксплуатации	Уметь обеспечивать информационную безопасность объектов информатизации в соответствии с правилами их эксплуатации
		ПК-4.3 Владеет навыками реализации защиты объектов информатизации в процессе их эксплуатации в соответствии с требованиями по информационной безопасности	Владеть навыками реализации защиты объектов информатизации в процессе их эксплуатации в соответствии с требованиями по информационной безопасности

2. Место модуля в структуре образовательной программы

Модуль входит в Вариативную часть.

Входные требования:

Предшествующие осваиваемые модули: Теоретические основы обработки сигналов, Защита информации от утечки по техническим каналам, Сети и системы передачи информации, Технологии и методы программирования;

Последующие осваиваемые модули: Выполнение и защита выпускной квалификационной работы.

3. Объем модуля в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Таблица 3

Вид учебной работы	Всего часов	В том числе часов в электронной форме	В том числе часов в форме практической подготовки	Семестр 1 часов/часов в электронной форме/в форме практической подготовки
Аудиторная контактная работа (всего), в том числе:	**40**	**0**	**0**	**40**
лекционные занятия (ЛЗ)	16	0	0	16
лабораторные работы (ЛР)	24	0	0	24
практические занятия (ПЗ)	0	0	0	0
Внеаудиторная контактная работа, КСР	**3**	**0**	**0**	**3**
Самостоятельная работа (всего), в том числе:	**65**	**0**	**0**	**65**
Подготовка к лабораторным работам	*65*	*0*	*0*	*65*
ИТОГО: час.	**108**	**0**	**0**	**108**
ИТОГО: з.е.	**3.0**	**0.0**	**0.0**	**3.0**

4. Содержание модуля, структурированное по темам (разделам), с указанием отведенного на них количества академических часов и видов учебных занятий

Таблица 4

№ раздела	Наименование раздела дисциплины	Виды учебной нагрузки и их трудоемкость, часы				
		ЛЗ	**ЛР**	**ПЗ**	**СРС**	**Всего часов**
1.	Нормативные основы информационно-аналитического мониторинга.	4	0	0	0	4
2.	Методология и организация информационно-аналитического мониторинга	12	24	0	65	101
	КСР					*3*
	Итого:	*16*	*24*	*0*	*65*	*108*

4.1. Содержание лекционных занятий

Таблица 4.1

№ ЛЗ	Наименование раздела	Тема лекции	Содержание лекции (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов	Количество часов в электронной форме
Семестр 1					
1.	Нормативные основы информационно-аналитического мониторинга.	Нормативная база информационно-аналитического мониторинга	Приказы ФСТЭК и ФСБ правительства России по теме.	2	0
2.	Нормативные основы информационно-аналитического мониторинга.	Моделирование угроз безопасности в системах информационно-аналитического мониторинга	Модели угроз, в том числе методика оценки угроз безопасности ФСТЭК.	2	0
3.	Методология и организация информационно-аналитического мониторинга	Межсетевое экранирование	Рассматривается классификация и механизм защиты межсетевых экранов.	2	0
4.	Методология и организация информационно-аналитического мониторинга	Сканеры уязвимостей	Назначение сканеров уязвимостей. Этапы проведения сканирования.	2	0
5.	Методология и организация информационно-аналитического мониторинга	Системы обнаружения и предотвращения вторжений (IDS/IPS)	Классификация, методы обнаружения и принципы размещения систем обнаружения и предотвращения вторжений.	2	0
6.	Методология и организация информационно-аналитического мониторинга	Мониторинг сети	Классификация средств мониторинга. Оборудование для мониторинга сетей.	2	0
7.	Методология и организация информационно-аналитического мониторинга	Управление событиями безопасности (SIEM)	Основные задачи, функции и классификация SIEM-систем.	2	0

№ ЛЗ	Наименование раздела	Тема лекции	Содержание лекции (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов	Количество часов в электронной форме
8.	Методология и организация информационно-аналитического мониторинга	Платформа реагирования на инциденты (IRP)	Основные задачи, функции и классификация IRP-систем	2	0
			Итого за семестр:	*16*	*0*
			Итого:	**16**	**0**

4.2. Содержание лабораторных занятий

Таблица 4.2

№ ЛабЗ	Наименование раздела	Наименование лабораторной работы	Содержание лабораторной работы (перечень рассматриваемых дидактических единиц: подтем, вопросов)	Количество часов	Количество часов в электронной форме	Количество часов в форме практической подготовки
Семестр 1						
1.	Методология и организация информационно-аналитического мониторинга	Межсетевое экранирование	Рассматривается классификация и механизм защиты межсетевых экранов.	4	0	*0*
2.	Методология и организация информационно-аналитического мониторинга	Сканеры уязвимостей	Назначение сканеров уязвимостей. Этапы проведения сканирования.	4	0	*0*
3.	Методология и организация информационно-аналитического мониторинга	Системы обнаружения и предотвращения вторжений (IDS/IPS)	Классификация, методы обнаружения и принципы размещения систем обнаружения и предотвращения вторжений.	4	0	*0*
4.	Методология и организация информационно-аналитического монитор	Мониторинг сети	Классификация средств мониторинга. Оборудование для мониторинга сетей.	4	0	*0*

№ ЛабЗ	Наименование раздела	Наименование лабораторной работы	Содержание лабораторной работы (перечень рассматриваемых дидактических единиц: подтем, вопросов)	Количество часов	Количество часов в электронной форме	Количество часов в форме практической подготовки
	инга					
5.	Методология и организация информационно-аналитического мониторинга	Управление событиями безопасности (SIEM)	Основные задачи, функции и классификация SIEM-систем.	4	0	*0*
6.	Методология и организация информационно-аналитического мониторинга	Платформа реагирования на инциденты (IRP)	Основные задачи, функции и классификация IRP-систем	4	0	*0*
			Итого за семестр:	*24*	*0*	*0*
			Итого:	**24**	**0**	***0***

4.3. Содержание самостоятельной работы

Таблица 4.4

Наименование раздела	Вид самостоятельной работы	Содержание самостоятельной работы (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов
Семестр 1			
Методология и организация информационно-аналитического мониторинга	Подготовка к лабораторным работам	Ознакомление с нормативными документами, а также с методологией и организацией информационно-аналитического мониторинга.	65
		Итого за семестр:	*65*
		Итого:	**65**

5. Перечень учебной литературы и учебно-методического обеспечения по модулю

Таблица 5

№ п/п	Библиографическое описание	Ссылка на ресурс
1.	Зегжда, Дмитрий Петрович Основы безопасности информационных систем : учеб. пособие для вузов по специальности "Компьютер. безопасность" и "Комплекс. обеспечение информ. безопасности автоматизир. систем" [Текст] .- Москва, Горячая линия - Телеком, 2000.- 451 с.	Книжный фонд АСА СамГТУ

Доступ обучающихся к ЭР НТБ СамГТУ (elib.samgtu.ru) осуществляется посредством электронной информационной образовательной среды университета и сайта НТБ СамГТУ по логину и паролю.

6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», профессиональных баз данных, информационно-справочных систем

Таблица 6

№ п/п	Наименование	Ссылка на веб-страницу ресурса	Режим доступа
1.	*Scopus: база данных рефератов и цитирования [Электронный ресурс]. - Электрон. текстовые, граф., зв. дан., Сайт в сети Интернет*	*http://www.scopus.com*	*Ресурсы ограниченного доступа*
2.	*eLIBRARY.RU (НЭБ - Научная электронная библиотека "Российский индекс научного цитирования") [Электронный ресурс]. - Электрон. текстовые, граф., зв. дан., Сайт в сети Интернет*	*http://www.elibrary.ru/*	*Ресурсы открытого доступа*
3.	*УИС РОССИЯ - Университетская информационная система РОССИЯ [Электронный ресурс]. - Электрон. текстовые, граф., зв. дан., Сайт в сети Интернет*	*http://www.cir.ru/*	*Ресурсы открытого доступа*

7. Описание материально-технической базы, необходимой для осуществления образовательного процесса по модулю

Лекционные занятия проводятся в:

Корпус № 8/111 - Учебная аудитория (Аудитория на 24 посадочных мест оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, столы учебные, доска аудиторная. Мультимедийное оборудование: проектор Acer Projector P1283; экран. Специализированное оборудование: стенд К-32 - 7шт., осциллограф С1-48Б - 5 шт., осциллограф С-93 - 2шт., осциллограф GRS-6052 - 1шт.).

Практические занятия не предусмотрены.

Самостоятельная работа проводятся в:

Корпус № 8/200 - Читальный зал (Аудитория на 70 посадочных мест оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, столы учебные.).

Лабораторные занятия проводятся в:

Корпус № 8/109 - Учебная лаборатория (Аудитория на 20 посадочных мест оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, столы учебные, доска аудиторная. Коммутатор D-Link DES-1016D. 10 ПК P4631\3.0GHz64bit2M в комплекте. На ПК установлено следующее программное обеспечение: операционная система MS Windows 7, офисный пакет MS Office 2007, Auto Cad, ЛИРА, антивирусное ESET nod 32, Auto CAD, PTC Mathcad Prime 3.1, ArchiCAD. Обеспечено проводное подключение ПК к локальной сети и сети Интернет.).

ПРИЛОЖЕНИЕ
Фонд оценочных средств

Фонд оценочных средств для текущего контроля успеваемости, промежуточной аттестации обучающихся по модулю

Настоящий Фонд оценочных средств (ФОС) по модулю Методология и организация информационно-аналитического мониторинга является неотъемлемым приложением к рабочей программе модуля. На данный ФОС распространяются все реквизиты утверждения, представленные в рабочей программе модуля.

1. Перечень оценочных средств

Таблица 1

№ п/п	Оценочное средство	Краткая характеристика оценочного средства	Количество	Представление оценочного средства в ФОС
1	Отчёт по лабораторной работе	Оценка способности студента применить полученные ранее знания для проведения анализа, опыта, эксперимента и выполнения последующих расчетов, а также составления выводов.	6	Требования к содержанию и оформлению отчета
2	Контрольная точка в форме тестирования	Инструмент, с помощью которого преподаватель оценивает степень достижения студентом требуемых знаний, умений, навыков в формате рубежного контроля по итогам изучения разделов. Составление теста включает в себя создание выверенной системы вопросов, собственно процедуру проведения тестирования и способ измерения полученных результатов.	1	Спецификация тестов и примеры вариантов тестовых заданий

Раздел 2. Этапы формирования компетенций, соотнесенные с видами оценочных средств

Таблица 2

Контролируемые разделы модуля	Код и формулировка индикатора компетенции	Результат обучения	Оценочные средства	Номер оценочного средства
Методология и организация информационно-аналитического мониторинга	ПК-4.1 Знает принципы работы и правила эксплуатации объектов информатизации, подлежащих защите	Знать принципы работы и правила эксплуатации объектов информатизации, подлежащих защите	Контрольная точка в форме тестирования	1
Методология и организация информационно-аналитического мониторинга	ПК-4.1 Знает принципы работы и правила эксплуатации объектов информатизации, подлежащих защите	Знать принципы работы и правила эксплуатации объектов информатизации, подлежащих защите	Отчёт по лабораторной работе	1-6

Методология и организация информационно-аналитического мониторинга	ПК-4.2 Умеет обеспечивать информационную безопасность объектов информатизации в соответствии с правилами их эксплуатации	Уметь обеспечивать информационную безопасность объектов информатизации в соответствии с правилами их эксплуатации	Отчёт по лабораторной работе	1-6
Методология и организация информационно-аналитического мониторинга	ПК-4.3 Владеет навыками реализации защиты объектов информатизации в процессе их эксплуатации в соответствии с требованиями по информационной безопасности	Владеть навыками реализации защиты объектов информатизации в процессе их эксплуатации в соответствии с требованиями по информационной безопасности	Отчёт по лабораторной работе	1-6

3. Содержание оценочных средств текущего контроля

Оценочное средство 1:
Пример отчета и вопросы по лабораторной работе прилагаются к программе модуля
Оценочное средство 2:
Пример тестов прилагается к программе модуля

4. Содержание оценочных средств промежуточной аттестации

Семестр 1:

Вид аттестационного испытания 1: Аттестация по результатам рейтинга (БРТ).
Форма проведения промежуточной аттестации: Зачет.
Типовые задания: .

5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций

Модуль состоит из набора разделов. Объем учебного раздела раскрывает отдельную (ые) тему(ы) модуля / этап прохождения практики. Модуль разбивается, как правило, на 2-4 раздела в семестр.

Раздел состоит из учебных элементов (дидактических единиц), сгруппированных по темам в рамках раздела. Объем учебного материала учебного элемента раскрывает отдельный вопрос темы. Путем набора соответствующих тем и учебных элементов формируется раздел, содержание которого соответствует запланированным результатам освоения ОП согласно учебному плану.

По каждому разделу устанавливается перечень обязательных видов работы студента, включающий: ответы на теоретические вопросы на семинаре; решение практических задач и выполнение заданий на практических занятиях; выполнение лабораторных работ; выполнение контрольных работ; написание рефератов; участие в коллоквиумах; тестирование по теме (группе тем); другие виды работ, определяемые преподавателем (в соответствии с установленными требованиями балльно-рейтинговой технологии).

Каждый раздел включает определенные формы контроля для оценки уровня усвоения учебного материала и определения рейтинговой оценки качества усвоения учебного материала.

Рейтинговая оценка знаний студентов определяется по 100-балльной шкале в каждом семестре и включает текущий, рубежный и итоговый контроль.

Накопленный рейтинг (фиксированная величина по окончании семестра) — это фактический рейтинг по всем освоенным к данному моменту разделам дисциплины, включая их текущий, рубежный и итоговый контроль, составляет N баллов (N – индивидуальная величина, зависящая от проделанной работы студента по дисциплине).

Проходной рейтинг (включает текущий контроль, рубежный контроль в семестре и промежуточную аттестацию) — это минимум баллов, набрав который студент будет считаться аттестованным по дисциплине, составляет __*(заполняется автоматически из справочника)* баллов в семестр по одной дисциплине.

Пороговый рейтинг (включает текущий контроль и рубежный контроль в семестре) — это минимальный фактический рейтинг семестрового контроля, набрав который, студент проходит на итоговый контроль, составляет 50% от суммы баллов, которые студент может набрать за текущий контроль и рубежный контроль в течение семестра.

Текущий контроль служит для получения первичной информации о ходе усвоения отдельных элементов содержания учебной дисциплины. Основное его назначение состоит в осуществлении контроля за всеми видами аудиторной и самостоятельной внеаудиторной деятельности студентов, результаты которого оцениваются в баллах.

Рубежный контроль (контрольные точки текущего контроля) проводится после изучения завершенной в смысловом и логическом плане части учебного материала (раздела, модуля). Этот вид контроля позволяет получить информацию о ходе усвоения некоторой совокупности содержательных элементов учебной дисциплины (раздела, модуля) и оценивается в баллах.

Промежуточный итоговый контроль (контрольные точки промежуточной аттестации) – курсовой проект, курсовая работа и экзамен, зачет, зачет с оценкой. Итоговый контроль по дисциплине в семестре предназначен для аттестации студента по учебной дисциплине: процедура установления соответствия уровня и качества подготовки студентов системе требований, зафиксированной в ФГОС ВО.

Распределение баллов рейтинговой оценки между видами контроля

Таблица 3

Форма промежуточной аттестации	Количество баллов			
	Текущий контроль	Рубежный контроль	Итоговый контроль	Сумма баллов
Зачет	0	0	5	5

Перевод оценок 100-балльной шкалы в оценки промежуточной аттестации

Таблица 4

100-балльная шкала	85-100	70-84	50-69	0-49
5-балльная шкала	Отлично	Хорошо	Удовлетворительно	Неудовлетворительно
Бинарная шкала	Зачтено			Не зачтено

Распределение рейтинговых баллов по разделам модуля с указанием применяемых для их начисления оценочных средств представлено в Технологической карте БРТ.

Технологическая карта БРТ

Семестр 1

Раздел учебного модуля	Оценочные средства			Итого
	Отчёт по лабораторной работе	**Контрольная точка в форме тестирования**	**Зачет**	
Раздел 1				
ЛЗ 1.1		0		0
ЛЗ 1.2		0		0
ЛЗ 1.3		23		23
ЛЗ 1.4		0		0
ЛЗ 1.5		0		0
ЛЗ 1.6		0		0
ЛР 1.1	4			4
ЛР 1.2	4			4
ЛР 1.3	4			4
ЛР 1.4	4			4
ЛР 1.5	4			4
ЛР 1.6	4			4
Итого по разделу 1	24	23		47
Промежуточная аттестация			5	5
Итого	24	23	5	52

Пример тестирования

1. Назовите 3 основных нормативных документа в области мониторинга информационной безопасности.
- a. ISO 27001
- b. Федеральный закон "О персональных данных"
- c. Федеральный закон "Об информации, информационных технологиях и о защите информации"

2. Что такое Threat-Intelligence?
- a. Информация о сетевых угрозах
- b. Документация по безопасности
- c. Информация об угрозах информационной безопасности

3. Опишите методику оценки угроз безопасности ФСТЭК.
- a. ФСТЭК - это федеральная служба России, не имеющая методику оценки угроз
- b. Методика оценки угроз безопасности ФСТЭК - это система оценки и классификации угроз безопасности информации
- c. ФСТЭК не имеет методику оценки угроз безопасности

4. Назовите основные источники событий в системах мониторинга информационной безопасности.
- a. Личные сообщения
- b. Журналы событий, сетевой трафик, антивирусные отчеты
- c. Газеты и журналы

5. Перечислите самые актуальные уязвимости ПО.
- a. Это изменяется со временем, и актуальные уязвимости могут меняться. Не существует постоянного списка.
- b. Heartbleed, Spectre, Meltdown
- c. Windows XP

6. Приведите структуру систем мониторинга информационной безопасности.
- a. Мониторинг событий, анализ событий, реагирование на события
- b. Мониторинг космической активности, анализ погоды, контроль за зоопарками
- c. Нет структуры

7. Назовите основные требования к средствам антивирусной защиты.
- a. Большой объем оперативной памяти
- b. Обязательное наличие физической кнопки "Выключить"
- c. Обновление базы вирусных сигнатур и проактивное обнаружение угроз

8. Роль и структура правил корреляций в SIEM-системах.
- a. Правила корреляции - это правила для анализа личных сообщений

- b. Правила корреляции в SIEM-системах определяют, какие события следует считать потенциальными угрозами, а структура включает в себя условия, действия и пороговые значения
- c. SIEM-системы не используют правила корреляции

9. Перечислите этапы проведения сканирования сканеров безопасности.
- a. Подключение к интернету, установка антивируса, запуск сканирования
- b. Подготовка, сканирование, анализ результатов, устранение уязвимостей
- c. Завершение работы

10. Что такое проблемы ложных срабатываний?
- a. Это проблемы с техникой ловли рыбы
- b. Ложные срабатывания - это события, которые ошибочно считаются угрозами безопасности, когда на самом деле нет угрозы
- c. Проблемы, связанные с переполнением журналов событий.

Примерный перечень вопросов для подготовки к лабораторным работам

1. Назовите 3 основных нормативных документа в области мониторинга информационной безопасности
2. Что такое Threat-Intelligence?
3. Опишите методику оценки угроз безопасности ФСТЭК
4. Назовите основные источники событий в системах мониторинга информационной безопасности.
5. Перечислите самые актуальные уязвимости ПО.
6. Приведите структуру систем мониторинга информационной безопасности.
7. Назовите основные требования к средствам антивирусной защиты.
8. Роль и структура правил корреляций в SIEM-системах.
9. Перечислите этапы проведения сканирования сканеров безопасности.
10. Что такое проблемы ложных срабатываний.

Содержание отчета по лабораторным работам

1. Цели и задачи лабораторной работы.
2. Краткое изложение теоретической части.
3. Принципиальные схемы и рисунки.
4. Таблицы экспериментальных значений и наблюдений.
5. Выводы по результатам работы.

Методические рекомендации при работе на лабораторном занятии

Проведение лабораторной работы делится на две условные части: теоретическую и практическую.

Необходимыми структурными элементами занятия являются проведение лабораторной работы, проверка усвоенного материала, включающая обсуждение теоретических основ выполняемой работы.

Перед лабораторной работой, как правило, проводится технико-теоретический инструктаж по использованию необходимого оборудования. Преподаватель корректирует деятельность обучающегося в процессе выполнения работы (при необходимости). После завершения лабораторной работы подводятся итоги, обсуждаются результаты деятельности.

Возможны следующие формы организации лабораторных работ: фронтальная, групповая и индивидуальная. При фронтальной форме выполняется одна и та же работа (при этом возможны различные варианты заданий). При групповой форме работа выполняется группой (командой). При индивидуальной форме обучающимися выполняются индивидуальные работы.

По каждой лабораторной работе имеются методические указания по их выполнению, включающие необходимый теоретический и практический материал, содержащие элементы и последовательную инструкцию по проведению выбранной работы, индивидуальные варианты заданий, требования и форму отчётности по данной работе.