Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 10.03.01 Информационная безопасность

Наименование образовательной программы: Безопасность компьютерных систем (продвинутый уровень)

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

Рабочая программа дисциплины
ТЕХНОЛОГИИ ПРОАКТИВНОЙ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Часть, формируемая участниками образовательных отношений**
№ дисциплины по учебному плану:	**Б1.Ч.11**
Трудоемкость в зачетных единицах:	**6 семестр - 5;**
Часов (всего) по учебному плану:	**180 часов**
Лекции	**6 семестр - 28 часа;**
Практические занятия	**6 семестр - 42 часа;**
Лабораторные работы	**не предусмотрено учебным планом**
Консультации	**проводится в рамках часов аудиторных занятий**
Самостоятельная работа	**6 семестр - 109,7 часов;**
в том числе на КП/КР	**не предусмотрено учебным планом**
Иная контактная работа	**проводится в рамках часов аудиторных занятий**
включая: **Отчет** **Контрольная работа** **Кейс (решение конкретных производственных ситуаций)** **Лабораторная работа**	
Промежуточная аттестация:	
Зачет с оценкой	**6 семестр - 0,3 часа;**

Москва 2022

ПРОГРАММУ СОСТАВИЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Поляк Р.И. Идентификатор: Rbc0e923e-PoliakRI-10208dd2	Р.И. Поляк
(должность)	(подпись)	(расшифровка подписи)

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Баронов О.Р. Идентификатор: R90d76356-BaronovOR-7bf8fd7e	О.Р. Баронов
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)
Заведующий выпускающей кафедры	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины: изучение технологий проактивной защиты и методов предотвращения воздействий на информационную систему

Задачи дисциплины

- получение знаний по устройству и принципу работы современных программных и программно-аппаратных средств защиты информации, использующих проактивные технологии;
- формирование представления о тенденциях развития проактивных технологий защиты и способов их применения в сфере информационной безопасности;
- получение навыков по проектированию, настройке и созданию контента систем защиты, использующих проактивные технологии.

Формируемые у обучающегося **компетенции** и запланированные **результаты обучения** по дисциплине, соотнесенные с **индикаторами достижения компетенций**:

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Запланированные результаты обучения**
ПК-2 Готов к внедрению систем защиты информации автоматизированных систем	ПК-2.З$_{ПК-2}$ Внедряет организационные меры по защите информации в автоматизированных системах	знать: - основные понятия и назначение технологий проактивной защиты, в т.ч. использующие перспективные технологии проактивной защиты; - основные виды, назначение и принцип работы современных средств защиты информации, использующих проактивные технологии и технологии реализации моделей безопасности компьютерных систем; - технологию создания правил, детектирующих угрозы безопасности современных компьютерных систем. уметь: - выбирать и применять средства защиты информации, использующих проактивные технологии, для нейтрализации угроз безопасности современных компьютерных систем; - анализировать причины нарушения функционирования средств защиты информации, использующих проактивные технологии; - внедрять организационные меры политик обновления системного и прикладного ПО, резервного копирования и управления уязвимостями; - применять навыки интеграции средств защиты информации, использующих проактивные технологии и автоматизации их настроек при выявлении угроз безопасности современных компьютерных систем;

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
		- применять навыки администрирования средств защиты информации, использующих проактивные технологии; - применять инструменты создания правил, детектирующих угрозы безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к основной профессиональной образовательной программе Безопасность компьютерных систем (продвинутый уровень) (далее – ОПОП), направления подготовки 10.03.01 Информационная безопасность, уровень образования: высшее образование - бакалавриат.

Базируется на уровне среднего общего образования.

Результаты обучения, полученные при освоении дисциплины, необходимы при выполнении выпускной квалификационной работы.

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единиц, 180 часов.

№ п/п	Разделы/темы дисциплины/формы промежуточной аттестации	Всего часов на раздел	Семестр	Распределение трудоемкости раздела (в часах) по видам учебной работы										Содержание самостоятельной работы/ методические указания
				Контактная работа								СР		
				Лек	Лаб	Пр	Консультация		ИКР		ПА	Работа в семестре	Подготовка к аттестации /контроль	
							КПР	ГК	ИККП	ТК				
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	Введение	10	6	2	-	4	-	-	-	-	-	4	-	***Изучение материалов литературных источников:*** [2], 8-15
1.1	Тема 1. Введение в проактивную защиту	10		2	-	4	-	-	-	-	-	4	-	
2	Проактивная защита конечных устройств (endpoint protection)	52		8	-	14	-	-	-	-	-	30	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Проактивная защита конечных устройств (endpoint protection)"
2.1	Тема 2. Организация проактивной защиты на базе защитных механизмов, встроенных в ОС (Windows, Linux).	10		2	-	2	-	-	-	-	-	6	-	***Подготовка расчетно-графического задания:*** В рамках расчетно-графического задания выполняется чертеж конструкции. Для выполнения чертежей выполняются предварительные расчеты основных показателей, которые указываются на чертеже. Задание выполняется индивидуально по вариантам. В качестве тем задания применяются следующие:
2.2	Тема 3. Технологии виртуализации в задачах проактивной защиты.	16		2	-	4	-	-	-	-	-	10	-	
2.3	Тема 4. Технологии эвристического детектирования и поведенческого анализа	20		2	-	6	-	-	-	-	-	12	-	***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы
2.4	Тема 5. Решения класса endpoint protection.	6		2	-	2	-	-	-	-	-	2	-	***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Проактивная защита конечных устройств (endpoint protection)" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры

														выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***<u>Подготовка доклада, выступления:</u>*** Задание связано с углубленным изучением разделов дисциплины и самостоятельным поиском материалов для раскрытия темы доклада. Материалы выполненной работы представляются в электронном виде или в форме распечатанных презентационных слайдов. В качестве тем докладов студентам предлагаются следующие варианты: ***<u>Подготовка к контрольной работе:</u>*** Изучение материалов по разделу Проактивная защита конечных устройств (endpoint protection) и подготовка к контрольной работе ***<u>Подготовка к практическим занятиям:</u>*** Изучение материала по разделу "Проактивная защита конечных устройств (endpoint protection)" подготовка к выполнению заданий на практических занятиях ***<u>Самостоятельное изучение теоретического материала:</u>*** Изучение дополнительного материала по разделу "Проактивная защита конечных устройств (endpoint protection)" ***<u>Изучение материалов литературных источников:</u>*** [3], 1-70 [4], 47-68 [5], 10-88 [6], 1-112 [7], 1-55 [8], 1-48
3	Проактивная защита сетевого периметра (network protection)	82		14	-	20	-	-	-	-	-	48	-	***<u>Подготовка к текущему контролю:</u>*** Повторение материала по разделу "Проактивная защита сетевого периметра

3.1	Тема 6. Технологии мониторинга и обнаружения событий в сети.	30		4	-	8	-	-	-	-	-	18	-	(network protection)" ***Подготовка к лабораторной работе:*** Для выполнения заданий по лабораторной работе необходимо предварительно изучить тему и задачи выполнения лабораторной работы, а так же изучить вопросы вариантов обработки результатов по изученному в разделе "Проактивная защита сетевого периметра (network protection)" материалу. ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Проактивная защита сетевого периметра (network protection)" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***Подготовка доклада, выступления:*** Задание связано с углубленным изучением разделов дисциплины и самостоятельным поиском материалов для раскрытия темы доклада. Материалы выполненной работы представляются в электронном виде или в форме распечатанных презентационных слайдов. В качестве тем докладов студентам предлагаются следующие варианты: ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Проактивная защита сетевого периметра (network protection)" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение***
3.2	Тема 7. Введение в threat hunting.	16		2	-	4	-	-	-	-	-	10	-	
3.3	Тема 8. Технология Threat Intelligence.	8		2	-	2	-	-	-	-	-	4	-	
3.4	Тема 9. Основы построения защищённых компьютерных сетей.	20		4	-	4	-	-	-	-	-	12	-	
3.5	Тема 10. Решения для защиты компьютерных сетей	8		2	-	2	-	-	-	-	-	4	-	

														теоретического материала: Изучение дополнительного материала по разделу "Проактивная защита сетевого периметра (network protection)" ***Изучение материалов литературных источников:*** [1], 50-334 [2], 56-210
4	Совершенствование проактивной защиты в ИС	18		4	-	4	-	-	-	-	-	10	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Совершенствование проактивной защиты в ИС" ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка доклада, выступления:*** Задание связано с углубленным изучением разделов дисциплины и самостоятельным поиском материалов для раскрытия темы доклада. Материалы выполненной работы представляются в электронном виде или в форме распечатанных презентационных слайдов. В качестве тем докладов студентам предлагаются следующие варианты: ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Совершенствование проактивной защиты в ИС" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Совершенствование проактивной защиты в ИС" ***Подготовка расчетных заданий:*** Задания ориентированы на решения минизадач по разделу "Совершенствование проактивной защиты в ИС". Студенты необходимо повторить теоретический материал,
4.1	Тема 11. Перспективные технологии проактивной защиты.	8		2	-	2	-	-	-	-	-	4	-	
4.2	Тема 12. Организационные меры проактивной защиты.	10		2	-	2	-	-	-	-	-	6	-	

														разобрать примеры решения аналогичных задач. провести расчеты по варианту задания и сделать выводы. В качестве задания используются следующие упражнения:
	Зачет с оценкой	18.0		-	-	-	-	-	-	-	0.3	-	17.7	
	Всего за семестр	**180.0**		**28**	**-**	**42**	**-**	**-**	**-**	**-**	**0.3**	**92**	**17.7**	
	Итого за семестр	**180.0**		**28**	**-**	**42**	**-**		**-**		**0.3**	**109.7**		

Примечание: Лек – лекции; Лаб – лабораторные работы; Пр – практические занятия; КПР – аудиторные консультации по курсовым проектам/работам; ИККП – индивидуальные консультации по курсовым проектам/работам; ГК- групповые консультации по разделам дисциплины; СР – самостоятельная работа студента; ИКР – иная контактная работа; ТК – текущий контроль; ПА – промежуточная аттестация

3.2 Краткое содержание разделов

1. Введение

1.1. Тема 1. Введение в проактивную защиту

Задачи курса. Реактивные и проактивные технологии защиты. История развития проактивных технологий защиты. Угрозы безопасности современных компьютерных систем..

2. Проактивная защита конечных устройств (endpoint protection)

2.1. Тема 2. Организация проактивной защиты на базе защитных механизмов, встроенных в ОС (Windows, Linux).

Основные защитные механизмы ОС Windows. Идентификация, аутентификация и авторизация. Разграничение доступа к объектам ОС. Архитектура ОС Windows. Кольца защиты. Компоненты безопасности Windows (Security Reference Monitor (SRM). Local Security Authority Subsystem Service (LSASS). Credential Providers. Windows Access Control. Malicious Credential Providers. Access Token. Impersonation. Privileges. Discretionary Access Control. Mandatory Integrity Control. User Account Control). Основные защитные механизмы ОС Linux (Пользователи и их права. Безопасное управление процессами. Работа с объектами файловой системы. Безопасность файловых систем EXT*FS. POSIX ACL. Sudo. Chroot. PAM. SELinux. AppArmor. PolicyKit)..

2.2. Тема 3. Технологии виртуализации в задачах проактивной защиты.

Основные понятия технологии виртуализации. Виртуализация серверов. Виртуализация на уровне операционных систем. Виртуализация сети. Виртуализация приложений. Виртуализация представлений. Виртуализация хранилищ. Гипервизор. Виртуальные машины. Sandbox, особенности реализации и функционирования, примеры. Эмуляция кода. Способы эмуляции. Примеры использования технологии для детектирования вредоносного ПО..

2.3. Тема 4. Технологии эвристического детектирования и поведенческого анализа

Эвристический анализ. Структура исполняемых файлов (PE, ELF). Детектирование исполняемых файлов (PE, ELF) с помощью эвристических алгоритмов. Технологии реализации эвристических алгоритмов. Yara. MalScan. Поведенческий анализ и детектирование. Ложные срабатывания, особенности выявления и обработки..

2.4. Тема 5. Решения класса endpoint protection.

Обзор вендоров и решений. Сравнительная характеристика решений. Примеры Use case’ов..

3. Проактивная защита сетевого периметра (network protection)

3.1. Тема 6. Технологии мониторинга и обнаружения событий в сети.

SIEM системы. Архитектура SIEM. Источники данных. Корреляция событий. Анализ стандартных журналов событий для выявления угрозы. Технологии сбора событий (winlogbeat, auditbeat, auditd). Расширенный аудит событий в системе (Sysmon). Технологии хранения и анализа событий (ELK stack). Системы honeypot, назначение, разновидности, сценарии использования. IDS/IPS системы, основные решаемые задачи. Технологии детектирования подозрительного трафика. IDS Suricata. IDS Suricata в IPS режиме. Технологии написания правил для IDS Suricata. Network Security Monitor (NSM) Zeek. Принцип работы. Особенности внедрения в корпоративную инфраструктуру..

3.2. Тема 7. Введение в threat hunting.

Обзор технологии проактивного поиска и обнаружения угроз. Модель зрелости использования Threat Hunting в информационной системе. Техники Threat Hunting. Источники информации и гипотез в Threat Hunting. Процесс проверки гипотез. Создание инфраструктуры для Threat Hunting..

3.3. Тема 8. Технология Threat Intelligence.

Обзор технологии. Сбор и аккумуляция данных. Обогащение полученных данных. Анализ. Внедрение результатов в информационную систему..

3.4. Тема 9. Основы построения защищённых компьютерных сетей.

Разновидности архитектур защищенных компьютерных сетей. Прокси сервера. Фильтрация сетевого трафика. NGFW. IP репутация. Доменная репутация. Особенности построения репутационных списков..

3.5. Тема 10. Решения для защиты компьютерных сетей

Обзор вендоров и решений. Сравнительная характеристика решений. Примеры Use case'ов..

4. Совершенствование проактивной защиты в ИС

4.1. Тема 11. Перспективные технологии проактивной защиты.

Data science в задачах ИБ. Введение в Машинное обучение. Обучение с учителем. Обучение без учителя. Метод Байеса. Кластеризация. Глубинное обучение..

4.2. Тема 12. Организационные меры проактивной защиты.

Оценка эффективности защиты периметра сети. Повышение осведомлённости сотрудников в области ИБ. Политика обновления системного и прикладного ПО. Политика резервного копирования. Управление уязвимостями..

3.3. Темы практических занятий

1. Сравнительная характеристика решений для защиты компьютерных.;
2. IP репутация. Доменная репутация. Особенности построения репутационных списков.;
3. Особенности внедрения технологии threat hunting в информационную систему.;
4. Интеграция IDS/IPS в компьютерную сеть.;
5. Подключение источников к SIEM системе и создание корреляционных правил.;
6. Угрозы современных компьютерных систем.;
7. Создание эвристических алгоритмов с помощью Yara;
8. Технология настройки защищенной виртуальной машины.;
9. Особенности практической реализации моделей безопасности компьютерных систем.;
10. Кластеризация данных в задачах ИБ.;
11. Интеграция SIEM в информационную систему.;
12. Создание плана осведомленности по вопросам ИБ.

3.4. Темы лабораторных работ

не предусмотрено

3.5 Консультации

Групповые консультации по разделам дисциплины (ГК)

1. Обсуждение материалов по кейсам раздела "Проактивная защита конечных устройств (endpoint protection)"
2. Обсуждение материалов по кейсам раздела "Проактивная защита сетевого периметра (network protection)"
3. Обсуждение материалов по кейсам раздела "Совершенствование проактивной защиты в ИС"

Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Проактивная защита конечных устройств (endpoint protection)"
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Проактивная защита сетевого периметра (network protection)"
3. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Совершенствование проактивной защиты в ИС"

3.6 Тематика курсовых проектов/курсовых работ

Курсовой проект/ работа не предусмотрены

3.7. Соответствие разделов дисциплины и формируемых в них компетенций

Запланированные результаты обучения по дисциплине (в соответствии с разделом 1)	Коды индикаторов	Номер раздела дисциплины (в соответствии с п.3.1)				Оценочное средство (тип и наименование)
		1	2	3	4	
Знать:						
технологию создания правил, детектирующих угрозы безопасности современных компьютерных систем	ПК-2.3$_{ПК-2}$		+	+		Отчет/Анализ угроз безопасности с использованием технологий проактивного поиска, обнаружения событий в сети и сбора событий с конечных устройств на основе ОС Windows.
основные виды, назначение и принцип работы современных средств защиты информации, использующих проактивные технологии и технологии реализации моделей безопасности компьютерных систем	ПК-2.3$_{ПК-2}$		+			Контрольная работа/Разработка архитектуры системы проактивной защиты в организации
основные понятия и назначение технологий проактивной защиты, в т.ч. использующие перспективные технологии проактивной защиты	ПК-2.3$_{ПК-2}$		+			Отчет/Изучение технологий эвристического детектирования и поведенческого анализа в контролируемой изолированной среде на основе ОС Windows
Уметь:						
применять инструменты создания правил, детектирующих угрозы безопасности	ПК-2.3$_{ПК-2}$		+	+		Лабораторная работа/Разработка эвристических алгоритмов с помощью Yara
применять навыки администрирования средств защиты информации, использующих проактивные технологии	ПК-2.3$_{ПК-2}$		+			Лабораторная работа/Практика применения технологии настройки защищенной виртуальной машины
применять навыки интеграции средств защиты информации, использующих проактивные технологии и автоматизации их настроек при выявлении угроз безопасности современных компьютерных систем	ПК-2.3$_{ПК-2}$			+		Лабораторная работа/Практика интеграции IDS/IPS в компьютерную сеть
внедрять организационные меры политик обновления системного и прикладного ПО, резервного	ПК-2.3$_{ПК-2}$				+	Отчет/Разработка плана осведомленности по вопросам ИБ

копирования и управления уязвимостями						
анализировать причины нарушения функционирования средств защиты информации, использующих проактивные технологии	ПК-2.3$_{ПК-2}$	+				Кейс (решение конкретных производственных ситуаций)/Разработка модели безопасности компьютерной системы
выбирать и применять средства защиты информации, использующих проактивные технологии, для нейтрализации угроз безопасности современных компьютерных систем	ПК-2.3$_{ПК-2}$			+		Отчет/Разработка корреляционных правил при использовании SIEM систем

4. КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ДИСЦИПЛИНЕ)

4.1. Текущий контроль успеваемости

6 семестр

Форма реализации: Выполнение задания

1. Анализ угроз безопасности с использованием технологий проактивного поиска, обнаружения событий в сети и сбора событий с конечных устройств на основе ОС Windows. (Отчет)
2. Изучение технологий эвристического детектирования и поведенческого анализа в контролируемой изолированной среде на основе ОС Windows (Отчет)
3. Разработка архитектуры системы проактивной защиты в организации (Контрольная работа)
4. Разработка модели безопасности компьютерной системы (Кейс (решение конкретных производственных ситуаций))
5. Разработка плана осведомленности по вопросам ИБ (Отчет)

Форма реализации: Компьютерное задание

1. Практика интеграции IDS/IPS в компьютерную сеть (Лабораторная работа)
2. Практика применения технологии настройки защищенной виртуальной машины (Лабораторная работа)
3. Разработка эвристических алгоритмов с помощью Yara (Лабораторная работа)

Форма реализации: Письменная работа

1. Разработка корреляционных правил при использовании SIEM систем (Отчет)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Зачет с оценкой (Семестр №6)

В диплом выставляется оценка за 6 семестр.

Примечание: Оценочные материалы по дисциплине приведены в фонде оценочных материалов ОПОП.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие для СПТУ по группе специальностей 2200 "Информатика и вычислительная техника" / В. Ф. Шаньгин . – М. : Форум : ИНФРА-М, 2011 . – 416 с. – (Профессиональное образование) . - ISBN 978-5-8199-0331-5 .;
2. Шаньгин В. Ф.- "Информационная безопасность", Издательство: "ДМК Пресс", Москва, 2014 - (702 с.)
http://e.lanbook.com/books/element.php?pl1_id=50578;

3. Таненбаум, Э. Современные операционные системы = Modern operating systems : пер. с англ. / Э. Таненбаум, Х. Бос . – 4-е изд . – Санкт-Петербург : Питер, 2021 . – 1120 с. – (Классика computer science) . - Тит. л. параллельн. англ. - ISBN 978-5-4461-1155-8 .;
4. Таненбаум, Э. Современные операционные системы = Modern operating systems : пер. с англ. / Э. Таненбаум, Х. Бос . – 4-е изд . – СПб. : Питер, 2018 . – 1120 с. – (Классика computer science) . - Тит. л. параллельн. англ. - ISBN 978-5-496-01395-6 .;
5. Котельников Е. В.- "Введение во внутреннее устройство Windows", (2-е изд.), Издательство: "ИНТУИТ", Москва, 2016 - (260 с.)
https://e.lanbook.com/book/100722;
6. Войтов, Н. М. Основы работы с Linux : учебный курс / Н. М. Войтов . – М. : ДМК, 2016 . – 216 с. - ISBN 978-5-94074-380-2 .;
7. Войтов Н. М.- "Основы работы с Linux. Учебный курс", Издательство: "ДМК Пресс", Москва, 2010 - (216 с.)
http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1198;
8. Войтов Н. М.- "Администрирование ОС Red Hat Enterprise Linux. Учебный курс", Издательство: "ДМК Пресс", Москва, 2011 - (192 с.)
http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1081.

5.2 Лицензионное и свободно распространяемое программное обеспечение:
1. СДО "Прометей";
2. Office / Российский пакет офисных программ;
3. Windows / Операционная система семейства Linux;
4. Майнд Видеоконференции;
5. Dr.Web;
6. Kali Linux;
7. Python;
8. ОС Linux.

5.3 Интернет-ресурсы, включая профессиональные базы данных и информационно-справочные системы:
1. **ЭБС Лань** - https://e.lanbook.com/
2. **ЭБС "Университетская библиотека онлайн"** - http://biblioclub.ru/index.php?page=main_ub_red
3. **Научная электронная библиотека** - https://elibrary.ru/
4. **Электронные ресурсы издательства Springer** - https://link.springer.com/
5. **База данных Web of Science** - http://webofscience.com/
6. **База данных Scopus** - http://www.scopus.com
7. **Национальная электронная библиотека** - https://rusneb.ru/
8. **ЭБС "Консультант студента"** - http://www.studentlibrary.ru/
9. **Журнал Science** - https://www.sciencemag.org/
10. **Электронная библиотека МЭИ (ЭБ МЭИ)** - http://elib.mpei.ru/login.php
11. **Информационно-справочная система «Кодекс/Техэксперт»** - Http:\\proinfosoft.ru; http://docs.cntd.ru/
12. **Открытая университетская информационная система «РОССИЯ»** - https://uisrussia.msu.ru

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных	Н-204, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, колонки

занятий и текущего контроля		звуковые, мультимедийный проектор, экран
	К-601, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, мультимедийный проектор, экран
Учебные аудитории для проведения практических занятий, КР и КП	М-503, Учебная лаборатория "Программно-аппаратная средства защиты информации"	парта, стол преподавателя, стул, шкаф для хранения инвентаря, компьютерная сеть с выходом в Интернет, доска маркерная, сервер, компьютер персональный, кондиционер
Учебные аудитории для проведения промежуточной аттестации	М-503, Учебная лаборатория "Программно-аппаратная средства защиты информации"	парта, стол преподавателя, стул, шкаф для хранения инвентаря, компьютерная сеть с выходом в Интернет, доска маркерная, сервер, компьютер персональный, кондиционер
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Помещения для самостоятельной работы	НТБ-303, Компьютерный читальный зал	стол компьютерный, стул, стол письменный, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, принтер, кондиционер
Помещения для консультирования	А-300, Учебная аудитория "А"	кресло рабочее, парта, стеллаж, стол преподавателя, стол учебный, стул, трибуна, микрофон, мультимедийный проектор, экран, доска маркерная, колонки, техническая аппаратура, кондиционер, телевизор
Помещения для хранения оборудования и учебного инвентаря	К-202/2, Склад кафедры БИТ	стеллаж для хранения инвентаря, стол, стул, шкаф для документов, шкаф для хранения инвентаря, тумба, запасные комплектующие для оборудования

Приложение А

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Технологии проактивной защиты информационных систем

(название дисциплины)

6 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

КМ-1 Практика применения технологии настройки защищенной виртуальной машины (Лабораторная работа)
КМ-1 Разработка модели безопасности компьютерной системы (Кейс (решение конкретных производственных ситуаций))
КМ-2 Разработка эвристических алгоритмов с помощью Yara (Лабораторная работа)
КМ-2 Изучение технологий эвристического детектирования и поведенческого анализа в контролируемой изолированной среде на основе ОС Windows (Отчет)
КМ-3 Разработка архитектуры системы проактивной защиты в организации (Контрольная работа)
КМ-3 Анализ угроз безопасности с использованием технологий проактивного поиска, обнаружения событий в сети и сбора событий с конечных устройств на основе ОС Windows. (Отчет)
КМ-3 Разработка корреляционных правил при использовании SIEM систем (Отчет)
КМ-4 Разработка плана осведомленности по вопросам ИБ (Отчет)
КМ-4 Практика интеграции IDS/IPS в компьютерную сеть (Лабораторная работа)

Вид промежуточной аттестации – Зачет с оценкой.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-1	КМ-2	КМ-2	КМ-3	КМ-3	КМ-3	КМ-4	КМ-4
		Неделя КМ:	4	4	8	8	12	12	12	15	15
1	Введение										
1.1	Тема 1. Введение в проактивную защиту			+							
2	Проактивная защита конечных устройств (endpoint protection)										
2.1	Тема 2. Организация проактивной защиты на базе защитных механизмов, встроенных в ОС (Windows, Linux).					+	+				
2.2	Тема 3. Технологии виртуализации в задачах проактивной защиты.		+			+	+				
2.3	Тема 4. Технологии эвристического детектирования и поведенческого анализа				+	+	+	+			

2.4	Тема 5. Решения класса endpoint protection.			+	+	+	+			
3	Проактивная защита сетевого периметра (network protection)									
3.1	Тема 6. Технологии мониторинга и обнаружения событий в сети.			+			+	+		+
3.2	Тема 7. Введение в threat hunting.			+			+			+
3.3	Тема 8. Технология Threat Intelligence.			+			+			+
3.4	Тема 9. Основы построения защищённых компьютерных сетей.									+
3.5	Тема 10. Решения для защиты компьютерных сетей									+
4	Совершенствование проактивной защиты в ИС									
4.1	Тема 11. Перспективные технологии проактивной защиты.								+	
4.2	Тема 12. Организационные меры проактивной защиты.								+	
	Вес КМ, %:	10	10	15	10	10	10	10	10	15