

Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 10.04.01 Информационная безопасность

Наименование образовательной программы: Управление информационной безопасностью

Уровень образования: высшее образование - магистратура

Форма обучения: Очная

Рабочая программа дисциплины
ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ
НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Блок:	Блок 1 «Дисциплины (модули)»
Часть образовательной программы:	Часть, формируемая участниками образовательных отношений
№ дисциплины по учебному плану:	Б4.Ч.02
Трудоемкость в зачетных единицах:	2 семестр - 2;
Часов (всего) по учебному плану:	72 часа
Лекции	2 семестр - 16 часов;
Практические занятия	не предусмотрено учебным планом
Лабораторные работы	не предусмотрено учебным планом
Консультации	проводится в рамках часов аудиторных занятий
Самостоятельная работа	2 семестр - 56 часа;
в том числе на КП/КР	не предусмотрено учебным планом
Иная контактная работа	проводится в рамках часов аудиторных занятий
включая: Контрольная работа Тестирование	
Промежуточная аттестация:	
Зачет	2 семестр - 0 часов;

Москва 2023

ПРОГРАММУ СОСТАВИЛ:

Преподаватель

(должность)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Капгер И.В.
	Идентификатор	R5d33df1e-KapgerIV-059b09ee

(подпись)

И.В. Капгер

(расшифровка
подписи)

СОГЛАСОВАНО:

Руководитель
образовательной программы

(должность, ученая степень, ученое звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Минзов А.С.
	Идентификатор	R17801759-MinzovAS-e8de8907

(подпись)

А.С. Минзов

(расшифровка
подписи)

Заведующий выпускающей
кафедры

(должность, ученая степень, ученое звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Невский А.Ю.
	Идентификатор	R4bc65573-NevskyAY-0b6e493d

(подпись)

А.Ю. Невский

(расшифровка
подписи)

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины: приобретение необходимых теоретических знаний и практических навыков по использованию принципов и методов защиты информации от несанкционированного доступа в автоматизированных системах (АС) и компьютерных сетях

Задачи дисциплины

- изучение способов и причин несанкционированного доступа к информации в АС;
- освоение методов создания систем аутентификации пользователей АС и компьютерных сетей;
- приобретение навыков использования методов оценки качества систем аутентификации.

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-1 Оценивание уровня безопасности компьютерных систем и сетей	ПК-1.3ПК-1 Проводит анализ безопасности компьютерных систем	знать: - методы оценки стоимости и уязвимости информации в компьютерных системах и сетях; - состав и методы оценки качества систем аутентификации пользователей компьютерных систем и сетей; - угрозы и способы несанкционированного доступа к информации в компьютерных системах и сетях и методы защиты от него. уметь: - обосновывать выбор системы аутентификации пользователей компьютерных систем и сетей; - использовать методы построения формальных моделей подсистем защиты информации автоматизированных систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к факультативным дисциплинам основной профессиональной образовательной программе Управление информационной безопасностью (далее – ОПОП), направления подготовки 10.04.01 Информационная безопасность, уровень образования: высшее образование - магистратура.

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 2 зачетных единицы, 72 часа.

№ 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	Угрозы и способы несанкционированного доступа к информации	22	2	4	-	-	-	-	-	-	-	18	-	<p><u>Подготовка к текущему контролю:</u> Повторение материала по разделу "Угрозы и способы несанкционированного доступа к информации"</p> <p><u>Подготовка к аудиторным занятиям:</u> Проработка лекции, выполнение и подготовка к защите лаб. работы</p> <p><u>Подготовка домашнего задания:</u> Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Угрозы и способы несанкционированного доступа к информации" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам.</p> <p><u>Самостоятельное изучение теоретического материала:</u> Изучение дополнительного материала по разделу "Угрозы и способы несанкционированного доступа к информации"</p> <p><u>Изучение материалов литературных источников:</u> [1], 1-272 [5], 6-41</p>
1.1	Понятие, угрозы, способы и причины несанкционированного доступа к информации	22		4	-	-	-	-	-	-	-	-	18	

2	Политики безопасности для компьютерных систем и способы их реализации	28		8	-	-	-	-	-	-	-	20	-	<u>Подготовка к текущему контролю:</u> Повторение материала по разделу "Политики безопасности для компьютерных систем и способы их реализации" <u>Подготовка к аудиторным занятиям:</u> Проработка лекции, выполнение и подготовка к защите лаб. работы
2.1	Определение и содержание политики безопасности для компьютерных систем	28		8	-	-	-	-	-	-	-	20	-	<u>Подготовка домашнего задания:</u> Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Политики безопасности для компьютерных систем и способы их реализации" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. <u>Самостоятельное изучение теоретического материала:</u> Изучение дополнительного материала по разделу "Политики безопасности для компьютерных систем и способы их реализации" <u>Изучение материалов литературных источников:</u> [2], 1-147 [3], 1-352
3	Системы аутентификации пользователей компьютерных систем и методы их построения	22		4	-	-	-	-	-	-	-	18	-	<u>Подготовка к текущему контролю:</u> Повторение материала по разделу "Системы аутентификации пользователей компьютерных систем и методы их построения" <u>Подготовка к аудиторным занятиям:</u> Проработка лекции, выполнение и подготовка к защите лаб. работы
3.1	Элементы, проблемы создания и использования систем аутентификации	22		4	-	-	-	-	-	-	-	18	-	<u>Подготовка домашнего задания:</u> Подготовка домашнего задания направлена на отработку умений решения

													профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Системы аутентификации пользователей компьютерных систем и методы их построения" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. <u>Самостоятельное изучение теоретического материала:</u> Изучение дополнительного материала по разделу "Системы аутентификации пользователей компьютерных систем и методы их построения" <u>Изучение материалов литературных источников:</u> [4], 1-88
	Зачет	-		-	-	-	-	-	-	-	-	-	
	Всего за семестр	72		16	-	-	-	-	-	-	-	56	
	Итого за семестр	72		16	-	-	-	-	-	-	-	56	

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. Угрозы и способы несанкционированного доступа к информации

1.1. Понятие, угрозы, способы и причины несанкционированного доступа к информации

Направления и основные способы защиты от несанкционированного доступа к информации. Ведение и защита регистрационной базы данных в компьютерных системах. Реализация угроз безопасности информации в компьютерных системах. Оценка ценности информации в компьютерных системах. Оценка уязвимости информации в компьютерных системах.

2. Политики безопасности для компьютерных систем и способы их реализации

2.1. Определение и содержание политики безопасности для компьютерных систем

Виды доступа к объектам компьютерной системы. Понятие монитора безопасности объектов. Дискреционная политика безопасности. Модель take-grant. Мандатная политика безопасности. Модель Белле-ЛаПадулы. Ролевая политика безопасности. Реализация политики безопасности. Понятия монитора безопасности субъектов и изолированной программной среды. Домены безопасности. Формальное доказательство правильности реализации политики безопасности. Практические методы построения изолированной программной среды. Контроль целостности объектов в компьютерной системе. Модель Биба. Генерация изолированной программной среды. Процедура доверенной загрузки операционной системы.

3. Системы аутентификации пользователей компьютерных систем и методы их построения

3.1. Элементы, проблемы создания и использования систем аутентификации

Стратегии выбора и атаки на системы аутентификации. Факторы аутентификации. Оценка распространенности и методы защиты от атак на системы аутентификации. Типовые шаблоны систем аутентификации. Сравнение типовых шаблонов аутентификации. Методы защиты в системах локальной аутентификации. Использование многоразовых паролей.

3.3. Темы практических занятий

не предусмотрено

3.4. Темы лабораторных работ

не предусмотрено

3.5 Консультации

Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Угрозы и способы несанкционированного доступа к информации"
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Политики безопасности для компьютерных систем и способы их реализации"
3. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Системы аутентификации пользователей компьютерных систем и методы их построения"

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	
Знать:					
угрозы и способы несанкционированного доступа к информации в компьютерных системах и сетях и методы защиты от него	ПК-1.3 _{ПК-1}	+			Тестирование/Тест №1 «Политики безопасности для компьютерных систем и теоретические основы их реализации»
состав и методы оценки качества систем аутентификации пользователей компьютерных систем и сетей	ПК-1.3 _{ПК-1}	+			Контрольная работа/Контрольная работа №1 «Понятие несанкционированного доступа к информации. Методы оценки стоимости и уязвимости информации в АС»
методы оценки стоимости и уязвимости информации в компьютерных системах и сетях	ПК-1.3 _{ПК-1}		+		Тестирование/Тест №2 «Элементы и шаблоны построения систем аутентификации пользователей АС»
Уметь:					
использовать методы построения формальных моделей подсистем защиты информации автоматизированных систем	ПК-1.3 _{ПК-1}	+			Тестирование/Тест №2 «Элементы и шаблоны построения систем аутентификации пользователей АС»
обосновывать выбор системы аутентификации пользователей компьютерных систем и сетей	ПК-1.3 _{ПК-1}			+	Контрольная работа/Контрольная работа №2 «Модели разграничения доступа к объектам компьютерных 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

2 семестр

Форма реализации: Письменная работа

1. Контрольная работа №1 «Понятие несанкционированного доступа к информации. Методы оценки стоимости и уязвимости информации в АС» (Контрольная работа)
2. Контрольная работа №2 «Модели разграничения доступа к объектам компьютерных систем» (Контрольная работа)
3. Тест №1 «Политики безопасности для компьютерных систем и теоретические основы их реализации» (Тестирование)
4. Тест №2 «Элементы и шаблоны построения систем аутентификации пользователей АС» (Тестирование)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Зачет (Семестр №2)

В диплом выставляется оценка за 2 семестр.

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

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Грушо, А. А. Теоретические основы компьютерной безопасности : учебное пособие для вузов по специальности 090100 "Информационная безопасность" / А. А. Грушо, Э. А. Применко, Е. Е. Тимонина . – М. : АКАДЕМИЯ, 2009 . – 272 с. – (Высшее профессиональное образование) . - ISBN 978-5-7695-4242-8 .;
2. Малюк, А. А. Введение в защиту информации в автоматизированных системах : учебное пособие по специальностям, не входящим в группу специальностей в области информационной безопасности / А. А. Малюк, С. В. Пазизин, Н. С. Погожин . – 3-е изд., стереотип . – М. : Горячая Линия-Телеком, 2005 . – 147 с. - ISBN 5-935170-62-0 .;
3. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие для вузов по направлению "Информационная безопасность" / П. Б. Хорев . – 2-е изд., испр. и доп . – М. : Форум : ИНФРА-М, 2017 . – 352 с. – (Высшее образование) . - ISBN 978-5-00091-004-7 .;
4. Хорев, П. Б. Защита информационных систем : учебное пособие по курсам "Защита информации", "Методы и средства защиты компьютерной информации" по направлениям "Прикладная математика и информатика", "Информационные системы и технологии" и "Прикладная информатика" / П. Б. Хорев, Моск. энерг. ин-т (МЭИ ТУ) . – М. : Издательский дом МЭИ, 2010 . – 88 с. - ISBN 978-5-383-00546-0 .
http://elib.mpei.ru/action.php?kt_path_info=ktcore.SecViewPlugin.actions.document&fDocumentId=1956;
5. Душкин А. В., Барсуков О. М., Кравцов Е. В., Славнов К. В.- "Программно-аппаратные средства обеспечения информационной безопасности", Издательство: "Горячая линия-

Телеком", Москва, 2018 - (248 с.)
<https://e.lanbook.com/book/111053>.

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.

5.3 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. Электронные ресурсы издательства Springer - <https://link.springer.com/>
4. База данных Web of Science - <http://webofscience.com/>
5. База данных Scopus - <http://www.scopus.com>
6. Национальная электронная библиотека - <https://rusneb.ru/>
7. ЭБС "Консультант студента" - <http://www.studentlibrary.ru/>
8. Журнал Science - <https://www.sciencemag.org/>
9. Электронная библиотека МЭИ (ЭБ МЭИ) - <http://elib.mpei.ru/login.php>
10. Портал открытых данных Российской Федерации - <https://data.gov.ru>
11. Электронная открытая база данных "Polpred.com Обзор СМИ" - <https://www.polpred.com>
12. Информационно-справочная система «Кодекс/Техэксперт» - <Http://proinfosoft.ru;>
<http://docs.cntd.ru/>
13. Открытая университетская информационная система «РОССИЯ» - <https://uisrussia.msu.ru>
14. Федеральный портал "Российское образование" - <http://www.edu.ru>

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	М-511, Учебная аудитория	парта, стол преподавателя, стул, доска меловая
	К-601, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, мультимедийный проектор, экран
Учебные аудитории для проведения промежуточной аттестации	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
	К-601, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, мультимедийный проектор, экран
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	М-511, Учебная аудитория	парта, стол преподавателя, стул, доска меловая
Помещения для хранения	К-202/2, Склад	стеллаж для хранения инвентаря, стол,

оборудования и учебного инвентаря	кафедры БИТ	стул, шкаф для документов, шкаф для хранения инвентаря, тумба, запасные комплектующие для оборудования
-----------------------------------	-------------	--

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Теоретические основы защиты информации от Несанкционированного доступа

(название дисциплины)

2 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

- КМ-1 Контрольная работа №1 «Понятие несанкционированного доступа к информации. Методы оценки стоимости и уязвимости информации в АС» (Контрольная работа)
- КМ-2 Тест №1 «Политики безопасности для компьютерных систем и теоретические основы их реализации» (Тестирование)
- КМ-3 Контрольная работа №2 «Модели разграничения доступа к объектам компьютерных систем» (Контрольная работа)
- КМ-4 Тест №2 «Элементы и шаблоны построения систем аутентификации пользователей АС» (Тестирование)

Вид промежуточной аттестации – Зачет.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	4	8	12	15
1	Угрозы и способы несанкционированного доступа к информации					
1.1	Понятие, угрозы, способы и причины несанкционированного доступа к информации		+	+		+
2	Политики безопасности для компьютерных систем и способы их реализации					
2.1	Определение и содержание политики безопасности для компьютерных систем					+
3	Системы аутентификации пользователей компьютерных систем и методы их построения					
3.1	Элементы, проблемы создания и использования систем аутентификации				+	
Вес КМ, %:			20	20	20	40