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

Направление подготовки/специальность: 38.03.05 Бизнес-информатика

Наименование образовательной программы: Информационное и программное обеспечение бизнес-процессов

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

Рабочая программа дисциплины
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Часть, формируемая участниками образовательных отношений**
№ дисциплины по учебному плану:	**Б1.Ч.07**
Трудоемкость в зачетных единицах:	**5 семестр - 5;**
Часов (всего) по учебному плану:	**180 часов**
Лекции	**5 семестр - 32 часа;**
Практические занятия	**5 семестр - 32 часа;**
Лабораторные работы	**не предусмотрено учебным планом**
Консультации	**проводится в рамках часов аудиторных занятий**
Самостоятельная работа	**5 семестр - 115,7 часов;**
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 с оценкой	**5 семестр - 0,3 часа;**

Москва 2022

ПРОГРАММУ СОСТАВИЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Крыжановский Ю.Е. Идентификатор: Rfbb7ca24-KryzhanovskyYY-e2b375	Ю.Е. Крыжановский
(должность)	(подпись)	(расшифровка подписи)

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Крепков И.М. Идентификатор: R04da5bdb-KrepkovIM-33fe3095	И.М. Крепков
(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 современных методов управления информационной безопасностью организации

Задачи дисциплины

- освоение теоретических основ обеспечения информационной безопасности на предприятии (в организации), а также в областях теории информации и системного анализа;
- формирование готовности и способности к активной профессиональной деятельности в условиях информационного противоборства;
- приобретение навыков правильного оформления результатов учебной деятельности.

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 Способность проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе	ИД-2$_{ПК-1}$ Выполняет сбор, систематизацию, документирование и анализ требований к информационным системам	знать: - особенности международного и федерального законодательства, регламентирующее информационную безопасность; - особенности системы поиска деловой и научной информации, связанные с информационной безопасностью; - регламенты, обеспечивающие защиту информации в специализированных системах и банках данных. уметь: - применять алгоритмы стандартных задач для поиска уязвимостей информационной системы организации; - разрабатывать обзоры, аннотации, рефераты, научные доклады, с учетом защиты информации; - использовать обзоры, аннотации, рефераты, научные доклады, для поиска уязвимостей информационной системы организации.
ПК-2 Способность участвовать в управлении жизненным циклом продуктов в области информационных технологий	ИД-2$_{ПК-2}$ Проводит обследование организаций, выявляет информационные потребности пользователей, формирует требования к информационной системе	знать: - функции и принципы информационной безопасности; - принципы, на которых базируется федеральное законодательство, регламентирующее информационную безопасность; - методы решения типовых задач, связанных с информационной безопасностью. уметь: - выстаивать систему защиты информации на основе принципов

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
		информационной безопасности; - искать уязвимости информационной системы организации; - использовать типовые ил стандартные задачи для обеспечения информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к основной профессиональной образовательной программе Информационное и программное обеспечение бизнес-процессов (далее – ОПОП), направления подготовки 38.03.05 Бизнес-информатика, 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	Современные проблемы информационной безопасности	46	5	8	-	12	-	-	-	-	-	26	-	***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Современные проблемы информационной безопасности" ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Современные проблемы информационной безопасности" подготовка к выполнению заданий на практических занятиях ***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: Современные и актуальные законы, стандарты и регламенты процесса обеспечения информационной безопасности. Термины и определения информационной безопасности. Руководящие документы, регламентирующие процесс управления информационной безопасностью. ***Подготовка домашнего задания:*** Подготовка домашнего задания направлена
1.1	Тема 1. Введение в информационную безопасность	12		2	-	4	-	-	-	-	-	6	-	
1.2	Тема 2. Основные термины информационной безопасности	16		2	-	4	-	-	-	-	-	10	-	
1.3	Тема 3. Законы, стандарты и регламенты процесса обеспечения информационной безопасности. Термины и определения.	18		4	-	4	-	-	-	-	-	10	-	

														на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Современные проблемы информационной безопасности" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка к текущему контролю:*** Повторение материала по разделу "Современные проблемы информационной безопасности" ***Подготовка реферата:*** В рамках реферативной части студенту необходим провести обзор литературных источников по выбранной теме, комплексно осветить вопрос в соответствии с темой реферата, подготовить презентацию для выступления по результатам работы на семинарском занятии. В качестве тем реферата студенту предлагаются следующие варианты: Современные и актуальные законы, стандарты и регламенты процесса обеспечения информационной безопасности. Термины и определения информационной безопасности. Руководящие документы, регламентирующие процесс управления информационной безопасностью. ***Изучение материалов литературных источников:*** [4], 26-93 [6], 112-145 [8], 35-93 [10], 15-84

2	Управление системой информационной безопасности	46		10	-	6	-	-	-	-	-	30	-	***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Управление системой информационной безопасности" ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Управление системой информационной безопасности" подготовка к выполнению заданий на практических занятиях ***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: Знакомство с организационными мерами обеспечения информационной безопасности. Особенности информационной безопасности критической информационной инфраструктуры. ***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Управление системой информационной безопасности" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка к лабораторной работе:*** Для
2.1	Тема 4. Место системы информационной безопасности организации	16		4	-	2	-	-	-	-	-	10	-	
2.2	Тема 5. Доктрина информационной безопасности Российской Федерации	14		2	-	2	-	-	-	-	-	10	-	
2.3	Тема 6. Модель информационной безопасности организации.	16		4	-	2	-	-	-	-	-	10	-	

														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 "Управление системой информационной безопасности" материалу. ***Подготовка к текущему контролю:*** Повторение материала по разделу "Управление системой информационной безопасности" ***Изучение материалов литературных источников:*** [1], 14-84 [3], 26-94 [6], 25-94 [7], 36-93 [10], 24-76
3	Меры обеспечения информационной безопасности	42		8	-	6	-	-	-	-	-	28	-	***Подготовка расчетных заданий:*** Задания ориентированы на решения минизадач по разделу "Меры обеспечения информационной безопасности". Студенты необходимо повторить теоретический материал, разобрать примеры решения аналогичных задач. провести расчеты по варианту задания и сделать выводы. В качестве задания используются следующие упражнения: ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Меры обеспечения информационной безопасности" ***Подготовка к контрольной работе:*** Изучение материалов по разделу Меры обеспечения информационной безопасности и подготовка к контрольной работе ***Подготовка доклада, выступления:*** Задание связано с углубленным изучением
3.1	Тема 7. Особенности информационной безопасности критической информационной инфраструктуры	14		2	-	2	-	-	-	-	-	10	-	
3.2	Тема 8. Криптографические методы обеспечения информационной безопасности	14		2	-	2	-	-	-	-	-	10	-	
3.3	Тема 9. Организация защиты от вредоносных программ (вирусов)	14		4	-	2	-	-	-	-	-	8	-	

														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: Знакомство с организационными мерами обеспечения информационной безопасности. Особенности информационной безопасности критической информационной инфраструктуры. ***Подготовка домашнего задания:*** Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Меры обеспечения информационной безопасности" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка к текущему контролю:*** Повторение материала по разделу "Меры обеспечения информационной безопасности" ***Изучение материалов литературных источников:*** [4], 45-136 [11], 26-112
4	Политики информационной безопасности	28		6	-	8	-	-	-	-	-	14	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Политики информационной безопасности"
4.1	Тема 10. Особенности защиты персональных	12		2	-	4	-	-	-	-	-	6	-	***Проведение исследований:*** Работа выполняется по индивидуальному заданию.

	данных												
4.2	Тема 11. Политика информационной безопасности	16		4	-	4	-	-	-	-	-	8	-

Для проведения исследования применяется следующие материалы: Управление политикой безопасности, назначение и структура политики информационной безопасности, особенности формирования политик информационной безопасности.
Подготовка реферата: В рамках реферативной части студенту необходим провести обзор литературных источников по выбранной теме, комплексно осветить вопрос в соответствии с темой реферата, подготовить презентацию для выступления по результатам работы на семинарском занятии. В качестве тем реферата студенту предлагаются следующие варианты:
Проведение эксперимента: Работа выполняется по индивидуальному заданию. Для проведения исследования применяется следующее оборудование: Управление политикой безопасности, назначение и структура политики информационной безопасности, особенности формирования политик информационной безопасности.
Подготовка к практическим занятиям: Изучение материала по разделу "Политики информационной безопасности" подготовка к выполнению заданий на практических занятиях
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 домашнего задания: Подготовка домашнего задания направлена на отработку умений решения

														профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Политики информационной безопасности" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. ***Изучение материалов литературных источников:*** [2], 24-63 [5], 24-112 [6], 145-168 [7], 45-84 [9], 56-82
	Зачет с оценкой	18.0		-	-	-	-	-	-	-	0.3	-	17.7	
	Всего за семестр	**180.0**		**32**	**-**	**32**	**-**	**-**	**-**	**-**	**0.3**	**98**	**17.7**	
	Итого за семестр	**180.0**		**32**	**-**	**32**	**-**		**-**		**0.3**	**115.7**		

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. Современные проблемы информационной безопасности

1.1. Тема 1. Введение в информационную безопасность

Введение в управление информационной безопасностью. Место информационной безопасности в экономических процессах. Выявление причин и следствий нарушения информационной безопасности. Проблемы, связанные с сотрудниками и техническими ресурсами..

1.2. Тема 2. Основные термины информационной безопасности

Термины информационной безопасности, регламентированные федеральным законодательством и стандартами. Особенности использования терминологии..

1.3. Тема 3. Законы, стандарты и регламенты процесса обеспечения информационной безопасности. Термины и определения.

Современные и актуальные законы, стандарты и регламенты процесса обеспечения информационной безопасности. Термины и определения информационной безопасности. Руководящие документы, регламентирующие процесс управления информационной безопасностью..

2. Управление системой информационной безопасности

2.1. Тема 4. Место системы информационной безопасности организации

Место системы информационной безопасности организации в системе безопасности Российской Федерации..

2.2. Тема 5. Доктрина информационной безопасности Российской Федерации

Доктрина информационной безопасности Российской Федерации как основного документа, представляющий собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере..

2.3. Тема 6. Модель информационной безопасности организации.

Моделирование процессов, связанных с информационной безопасности организации. Использование описательных шаблонов, автоматизация процесса моделирования. Документы, регламентирующие процесс управления информационной безопасностью..

3. Меры обеспечения информационной безопасности

3.1. Тема 7. Особенности информационной безопасности критической информационной инфраструктуры

Знакомство с организационными мерами обеспечения информационной безопасности. Особенности информационной безопасности критической информационной инфраструктуры..

3.2. Тема 8. Криптографические методы обеспечения информационной безопасности

Варианты использования криптографических методов обеспечения информационной безопасности при формировании проектов..

3.3. Тема 9. Организация защиты от вредоносных программ (вирусов)

Методы и варианты организации защиты от вредоносных программ (вирусов). Классификация вирусов. Система защиты от вирусов..

4. Политики информационной безопасности

4.1. Тема 10. Особенности защиты персональных данных

Особенности защиты персональных данных. Требования федерального законодательства. Классификация информационных систем персональных данных..

4.2. Тема 11. Политика информационной безопасности

Управление политикой безопасности, назначение и структура политики информационной безопасности, особенности формирования политик информационной безопасности..

3.3. Темы практических занятий

1. Место системы информационной безопасности организации в системе безопасности Российской Федерации;
2. Модель информационной безопасности организации;
3. Вредоносные программы и защита от них. Организация защиты от вредоносных программ (вирусов);
4. Криптографические методы обеспечения информационной безопасности;
5. Организационные меры защиты информации;
6. Проведение анализа рисков;
7. Политика информационной безопасности. Управление политикой безопасности;
8. Особенности защиты персональных данных. Требования федерального законодательства. Особенности защиты персональных данных;
9. Законы, стандарты и регламенты процесса обеспечения информационной безопасности. Термины и определения;
10. Моделирование процессов, связанных с ИБ. Создание моделей нарушителя и актуальных угроз безопасности информационной;
11. Современные проблемы информационной безопасности. Введение в управление информационной безопасностью;
12. Система защиты компьютера с использованием паролей;
13. Каналы доступа к информации;
14. Документы, регламентирующие процесс управления информационной безопасностью.

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 "Современные проблемы информационной безопасности"
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Управление системой информационной безопасности"

3. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Меры обеспечения информационной безопасности"
4. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Политики информационной безопасности"

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:						
регламенты, обеспечивающие защиту информации в специализированных системах и банках данных	ИД-2$_{ПК-1}$	+				Контрольная работа/КМ-1
особенности системы поиска деловой и научной информации, связанные с информационной безопасностью	ИД-2$_{ПК-1}$	+				Тестирование/КМ-2
особенности международного и федерального законодательства, регламентирующее информационную безопасность	ИД-2$_{ПК-1}$	+				Тестирование/КМ-2
методы решения типовых задач, связанных с информационной безопасностью	ИД-2$_{ПК-2}$			+		Тестирование/КМ-3
принципы, на которых базируется федеральное законодательство, регламентирующее информационную безопасность	ИД-2$_{ПК-2}$		+			Тестирование/КМ-3
функции и принципы информационной безопасности	ИД-2$_{ПК-2}$		+			Тестирование/КМ-2
Уметь:						
использовать обзоры, аннотации, рефераты, научные доклады, для поиска уязвимостей информационной системы организации	ИД-2$_{ПК-1}$				+	Тестирование/КМ-4
разрабатывать обзоры, аннотации, рефераты, научные доклады, с учетом защиты информации	ИД-2$_{ПК-1}$			+		Тестирование/КМ-3
применять алгоритмы стандартных задач для поиска уязвимостей информационной системы организации	ИД-2$_{ПК-1}$			+		Тестирование/КМ-3
использовать типовые ил стандартные задачи для обеспечения информационной безопасности	ИД-2$_{ПК-2}$		+			Тестирование/КМ-3
искать уязвимости информационной системы организации	ИД-2$_{ПК-2}$				+	Тестирование/КМ-4
выстаивать систему защиты информации на основе принципов информационной безопасности	ИД-2$_{ПК-2}$				+	Тестирование/КМ-4

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

4.1. Текущий контроль успеваемости

5 семестр

Форма реализации: Компьютерное задание

1. КМ-1 (Контрольная работа)
2. КМ-2 (Тестирование)
3. КМ-3 (Тестирование)
4. КМ-4 (Тестирование)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Зачет с оценкой (Семестр №5)

5 семестр Зачет с оценкой. Оценка определяется по совокупности результатов текущего контроля успеваемости в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ».

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

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Аминев, А. В. Измерения в телекоммуникационных системах : учебное пособие для студентов , обучающихся по специальности "Информационная безопасность телекоммуникационных систем" / А. В. Аминев, А. В. Блохин ; общ. ред. А. В. Блохин ; Уральский федерал. ун-т им. первого Президента России Б.Н. Ельцина . – Москва : Юрайт, 2020 . – 223 с. – (Высшее образование) . - ISBN 978-5-534-05138-4 .;
2. Минзов, А. С. Управление рисками информационной безопасности : [монография] / А. С. Минзов, А. Ю. Невский, О. Р. Баронов ; ред. А. С. Минзов ; Нац. исслед. ун-т "МЭИ" (НИУ"МЭИ"), Инженерно-экономич. ин-т национального исслед. ун-та "МЭИ", Кафедра "Безопасности и Информационных Технологий" (БИТ) . – Москва : ВНИИгеосистем, 2019 . – 106 с. - ISBN 978-5-8481-0240-6 .;
3. Агуреев, И. А. Инженерно-техническая защита информации. Ч. 3 : учебное пособие и лабораторный практикум для Инженерно-экономического института / И. А. Агуреев, А. Ю. Невский, С. С. Рыжиков, Инженерно-экономич. ин-т национального исслед. ун-та "МЭИ" . – Москва : ВНИИгеосистем, 2021 . – 98 с. - ISBN 978-5-8481-0250-5 .;
4. Невский, А. Ю. Инженерно-техническая защита информации. Лабораторный практикум. Ч.2 : учебное пособие для Инженерно-экономического ин-та / А. Ю. Невский, О. Р. Баронов, А. С. Васильев, Инженерно-экономич. ин-т национального исслед. ун-та "МЭИ" . – М. : ВНИИгеосистем, 2017 . – 140 с. - ISBN 978-5-8481-0221-5 .;
5. Невский, А. Ю. Система обеспечения информационной безопасности хозяйствующего субъекта : учебное пособие / А. Ю. Невский, О. Р. Баронов ; Ред. Л. М. Кунбутаев ; Моск. энерг. ин-т (МЭИ ТУ) . – М. : Издательский дом МЭИ, 2009 . – 372 с. - ISBN 978-5-383-00375-6 .
http://elib.mpei.ru/action.php?kt_path_info=ktcore.SecViewPlugin.actions.document&fDocumentId=1468;

6. Гаранин, М. В. Системы и сети передачи информации : Учебное пособие для вузов по специальности "Криптография", "Компьютерная безопасность", "Комплексное обеспечение информационной безопасности автоматизированных систем", "Информационная безопасность телекоммуникационных систем" / М. В. Гаранин, В. И. Журавлев, С. В. Кунегин . – М. : Радио и связь, 2001 . – 336 с. - ISBN 5-256-01475-7 .;
7. А. А. Анисимов- "Менеджмент в сфере информационной безопасности: курс лекций", Издательство: "Интернет-Университет Информационных Технологий (ИНТУИТ)|Бином. Лаборатория знаний", Москва, 2009 - (176 с.)
https://biblioclub.ru/index.php?page=book&id=232981;
8. "Вопросы безопасности в Lotus Notes и Domino 7: курс", Издательство: "Интернет-Университет Информационных Технологий (ИНТУИТ)", Москва, 2008 - (305 с.)
https://biblioclub.ru/index.php?page=book&id=234895;
9. Д. В. Ковалев, Е. А. Богданова- "Информационная безопасность", Издательство: "Южный федеральный университет", Ростов-на-Дону, 2016 - (74 с.)
https://biblioclub.ru/index.php?page=book&id=493175;
10. Малюк А. А., Горбатов В. С., Королев В. И., Фомичев В. М., Дураковский А. П., Кондратьева Т. А.- "Введение в информационную безопасность", Издательство: "Горячая линия-Телеком", Москва, 2018 - (288 с.)
https://e.lanbook.com/book/111075;
11. Ю. Ю. Громов, Ю. Ф. Мартемьянов, Ю. К. Букурако, О. Г. Иванова, В. Г. Однолько- "Организация безопасной работы информационных систем", Издательство: "Тамбовский государственный технический университет (ТГТУ)", Тамбов, 2014 - (132 с.)
https://biblioclub.ru/index.php?page=book&id=277794.

5.2 Лицензионное и свободно распространяемое программное обеспечение:
1. СДО "Прометей";
2. Office;
3. Windows;
4. Acrobat;
5. Майнд Видеоконференции;
6. Dr.Web;
7. Access;
8. SAS Studio;
9. 1С: Предприятие 8. Версия для обучения программированию.

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. **База данных ВИНИТИ online** - http://www.viniti.ru/
5. **База данных журналов издательства Elsevier** - https://www.sciencedirect.com/
6. **Электронные ресурсы издательства Springer** - https://link.springer.com/
7. **База данных Web of Science** - http://webofscience.com/
8. **База данных Scopus** - http://www.scopus.com
9. **Национальная электронная библиотека** - https://rusneb.ru/
10. **ЭБС "Консультант студента"** - http://www.studentlibrary.ru/
11. **Журналы American Chemical Society** - https://www.acs.org/content/acs/en.html
12. **База данных издательства Annual Reviews Science Collection** - https://www.annualreviews.org/

13. **База данных IEL издательства IEEE (Institute of Electrical and Electronics Engineers, Inc.)** - https://ieeexplore.ieee.org/Xplore/home.jsp?reload=true
14. **Журналы Institute of Physics (IOP), Великобритания** - https://iopscience.iop.org/
15. **Журналы по химии Thieme Chemistry Package компании Georg Thieme Verlag KG** - https://www.thieme-connect.com/products/all/home.html
16. **Электронная библиотека МЭИ (ЭБ МЭИ)** - http://elib.mpei.ru/login.php
17. **База открытых данных Министерства экономического развития РФ** - http://www.economy.gov.ru
18. **Электронная открытая база данных "Polpred.com Обзор СМИ"** - https://www.polpred.com
19. **Информационно-справочная система «Кодекс/Техэксперт»** - Http:\\proinfosoft.ru; http://docs.cntd.ru/
20. **Официальный сайт Федерального агентства по техническому регулированию и метрологии** - http://protect.gost.ru/
21. **Открытая университетская информационная система «РОССИЯ»** - https://uisrussia.msu.ru
22. **Официальный сайт Министерства науки и высшего образования Российской Федерации** - https://minobrnauki.gov.ru
23. **Официальный сайт Федеральной службы по надзору в сфере образования и науки** - https://obrnadzor
24. **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	К-601, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, мультимедийный проектор, экран
	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
Учебные аудитории для проведения практических занятий, КР и КП	К-204а, Учебная лаборатория “Оракл-ФОРС”	стол преподавателя, стол компьютерный, стол учебный, стул, шкаф для одежды, мультимедийный проектор, экран, доска маркерная, компьютер персональный, кондиционер, телевизор
Учебные аудитории для проведения промежуточной аттестации	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
	К-204а, Учебная лаборатория “Оракл-ФОРС”	стол преподавателя, стол компьютерный, стол учебный, стул, шкаф для одежды, мультимедийный проектор, экран, доска маркерная, компьютер персональный, кондиционер, телевизор
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	А-300, Учебная	кресло рабочее, парта, стеллаж, стол

консультирования	аудитория "А"	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

Информационная безопасность

(название дисциплины)

5 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:
КМ-1 КМ-1 (Контрольная работа)
КМ-2 КМ-2 (Тестирование)
КМ-3 КМ-3 (Тестирование)
КМ-4 КМ-4 (Тестирование)

Вид промежуточной аттестации – Зачет с оценкой.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	4	8	12	15
1	Современные проблемы информационной безопасности					
1.1	Тема 1. Введение в информационную безопасность		+			
1.2	Тема 2. Основные термины информационной безопасности		+			
1.3	Тема 3. Законы, стандарты и регламенты процесса обеспечения информационной безопасности. Термины и определения.			+		
2	Управление системой информационной безопасности					
2.1	Тема 4. Место системы информационной безопасности организации			+		
2.2	Тема 5. Доктрина информационной безопасности Российской Федерации				+	
2.3	Тема 6. Модель информационной безопасности организации.				+	
3	Меры обеспечения информационной безопасности					
3.1	Тема 7. Особенности информационной безопасности критической информационной инфраструктуры				+	
3.2	Тема 8. Криптографические методы обеспечения информационной безопасности				+	
3.3	Тема 9. Организация защиты от вредоносных программ (вирусов)				+	
4	Политики информационной безопасности					
4.1	Тема 10. Особенности защиты персональных данных					+

4.2	Тема 11. Политика информационной безопасности				+
	Вес КМ, %:	25	25	25	25