Калужский филиал
федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)»
(КФ МГТУ им. Н.Э. Баумана)

Кафедра ИУК6 «Защита информации»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Основы информационной безопасности

Автор программы:
Лачихина А.Б., доцент (к.н.), кандидат технических наук, доцент, lachikhinaab@bmstu.ru

Утверждена на заседании кафедры «Защита информации»
Протокол № 07.04.06-04.08/4 от 04.04.2024 г.

ОГЛАВЛЕНИЕ

с.

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Настоящая рабочая программа дисциплины устанавливает требования к знаниям и умениям студента, а также определяет содержание и виды учебных занятий и отчетности.

Программа разработана в соответствии с:

• Самостоятельно устанавливаемыми образовательными стандартами (СУОС 3++) по специальностям (уровень специалитета): 10.05.03 «Информационная безопасность автоматизированных систем», 10.05.05 «Безопасность информационных технологий в правоохранительной сфере»;

• Основными профессиональными образовательными программами по специальностям 10.05.03 «Информационная безопасность автоматизированных систем», 10.05.05 «Безопасность информационных технологий в правоохранительной сфере»;

• Учебными планами МГТУ им. Н.Э. Баумана по специальностям 10.05.03 «Информационная безопасность автоматизированных систем», 10.05.05 «Безопасность информационных технологий в правоохранительной сфере».

При освоении дисциплины планируется формирование компетенций, предусмотренных основной профессиональной образовательной программой (ОПОП) на основе СУОС 3++ по специальностям 10.05.03 «Информационная безопасность автоматизированных систем», 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» (уровень специалитета)

Шифр компетенции, код направления подготовки/специальности по СУОС 3++	**Формулировка компетенции**
	Общепрофессиональные компетенции собственные
ОПКС-1 (10.05.03)	Способен понимать и оценивать роль информации, информационных технологий и информационной безопасности в развитии современного общества, оценивать их значение для обеспечения объективных потребностей личности, общества и государства
ОПКС-5 (10.05.05)	Способен планировать проведение работ по комплексной защите информации на объекте информатизации
ОПКС-5 (10.05.03)	Способен применять нормативные правовые акты, нормативно-методические и организационно распорядительные документы, международные и национальные стандарты в области своей профессиональной деятельности
ОПКС-6 (10.05.03)	Способен осуществлять проверку выполнения требований и организовать защиту информации в автоматизированных системах в соответствии с нормативными правовыми актами Российской Федерации, нормативными и методическими документами ФСБ России и ФСТЭК России, а также в соответствии с международными стандартами в области информационной безопасности
ОПКС-8 (10.05.03)	Способен вести научно-исследовательскую работу, разрабатывать технические задания на создание эскизных и технических проектов, выполнять анализ научно-технической информации, использовать методы и применять результаты

	научных исследований для решения задач в области профессиональной деятельности, оформлять по результатам проведенных исследований научно-технические отчеты, обзоры и публикации
ОПКС-8 (10.05.05)	Способен реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз
ОПКС-14 (10.05.03)	Способен осуществлять разработку, внедрение и эксплуатацию автоматизированной системы с учетом требований информационной безопасности и составлять технико-экономического обоснование проектных решений, включая подготовку исходных данных, и техническое задание на разработку системы защиты информации, а также способен выявлять недостатки существующих автоматизированных систем в соответствии с требованиями по защите информации
ОПКС-16 (10.05.03)	Способен исследовать современные проблемы информационной безопасности, анализировать процессы развития информационного общества, учитывая анализ основных этапов и закономерностей исторического развития России, ее место и роль в современном мире, в том числе для формирования гражданской позиции и развития патриотизма
ОПКС-19 (10.05.03)	Способен участвовать в разработке средств защиты информации подсистем обеспечения информационной безопасности в автоматизированных системах критически важных объектов
ОПКС-20 (10.05.03)	Способен организовать и обеспечить информационную безопасность при реализации технологических и бизнес-процессов организаций кредитно-финансовой сферы, в том числе процессов, связанных с осуществлением переводов денежных средств
ОПКС-25 (10.05.03)	Способен планировать и проводить анализ защищенности и верификацию программного обеспечения информационных систем
ОПКС-27 (10.05.03)	Способен участвовать в проектировании системы управления информационной безопасностью автоматизированной системы в защищенном исполнении
	Профессиональные компетенции собственные
ПКС-6 (10.05.03/41 Анализ безопасности информационных систем)	Способен участвовать в разработке требований по защите, формировании политик безопасности компьютерных систем и сетей

Для освоения компетенций, входящих в ОПОП, предусмотрены следующие индикаторы достижения компетенций (таблица 1).

Таблица 1. Индикаторы достижения компетенции

1	2	3
Шифр компетенции, код направления подготовки/специальности по СУОС 3++, формулировка	**Индикаторы достижения компетенции**	**Формы и методы обучения, способствующие формированию и развитию компетенции**
ОПКС-1 (10.05.03) Способен понимать и оценивать роль информации, информационных технологий и информационной безопасности в развитии современного общества, оценивать их значение для обеспечения объективных потребностей личности, общества и государства	ЗНАТЬ - понятие безопасности и её составляющих - содержание и структуру понятия обеспечения информационной безопасности УМЕТЬ - понимать значение информации в развитии современного общества	**Формы обучения:** Фронтальная и групповая формы. **Методы обучения:** Словесный метод обучения (Лекции) Наблюдение и Исследовательский метод (Лабораторные работы) Метод проблемного обучения(Самостоятельная работа) **Активные и интерактивные методы обучения:** обсуждение практических примеров на лекциях
ОПКС-5 (10.05.05) Способен планировать проведение работ по комплексной защите информации на объекте информатизации	ЗНАТЬ - классификацию объектов информатизации, их инженерно-техническое устройство и особенности технологического функционирования, виды угроз безопасности информации и основные способы их реализации, особенности функционирования объекта защиты в период реализации угроз, действия персонала по их нейтрализации и восстановлению нормального функционирования - понятие, виды, форму и содержание планов по проведению работ по комплексной защите информации на объекте информатизации, методы и средства планирования проведения работ по комплексной защите информации на объекте информатизации УМЕТЬ	**Формы обучения:** Фронтальная и групповая формы. **Методы обучения:** Словесный метод обучения (Лекции) Наблюдение и Исследовательский метод (Лабораторные работы) Метод проблемного обучения(Самостоятельная работа) **Активные и интерактивные методы обучения:** обсуждение практических примеров на лекциях

1	2	3
	- определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты, разрабатывать отдельные планы по проведению работ по комплексной защите информации на объекте информатизации, применять методы и средства планирования проведения этих работ ВЛАДЕТЬ - навыками участия в работах по планированию проведения работ по комплексной защите информации на объекте информатизации	
ОПКС-5 (10.05.03) Способен применять нормативные правовые акты, нормативно-методические и организационно распорядительные документы, международные и национальные стандарты в области своей профессиональной деятельности	УМЕТЬ - проводить поиск нормативной правовой информации необходимой для профессиональной деятельности	**Формы обучения:** Фронтальная и групповая формы. **Методы обучения:** Словесный метод обучения (Лекции) Наблюдение и Исследовательский метод (Лабораторные работы) Метод проблемного обучения(Самостоятельная работа) **Активные и интерактивные методы обучения:** обсуждение практических примеров на лекциях
ОПКС-6 (10.05.03) Способен осуществлять проверку выполнения требований и организовать защиту информации в автоматизированных системах в соответствии с нормативными	ЗНАТЬ - угрозы безопасности информации и их классификацию - виды мероприятий по защите информации, классификация методов и способов защиты информации объектов информатизации	**Формы обучения:** Фронтальная и групповая формы. **Методы обучения:** Словесный метод обучения (Лекции) Наблюдение и Исследовательский метод (Лабораторные работы) Метод проблемного обучения(Самостоятельная работа)

1	2	3
правовыми актами Российской Федерации, нормативными и методическими документами ФСБ России и ФСТЭК России, а также в соответствии с международными стандартами в области информационной безопасности		**Активные и интерактивные методы обучения:** обсуждение практических примеров на лекциях
ОПКС-8 (10.05.03) Способен вести научно-исследовательскую работу, разрабатывать технические задания на создание эскизных и технических проектов, выполнять анализ научно-технической информации, использовать методы и применять результаты научных исследований для решения задач в области профессиональной деятельности, оформлять по результатам проведенных исследований научно-технические отчеты, обзоры и публикации	ВЛАДЕТЬ - навыками обработки научно-технической информации в области защиты информации	**Формы обучения:** Фронтальная и групповая формы. **Методы обучения:** Словесный метод обучения (Лекции) Наблюдение и Исследовательский метод (Лабораторные работы) Метод проблемного обучения(Самостоятельная работа) **Активные и интерактивные методы обучения:** обсуждение практических примеров на лекциях
ОПКС-8 (10.05.05) Способен реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную	ЗНАТЬ - понятие и классификацию по требованиям безопасности информации объектов информатизации, обрабатывающих информацию, относимую действующим законодательством Российской Федерации к государственной тайне и	**Формы обучения:** Фронтальная и групповая формы. **Методы обучения:** Словесный метод обучения (Лекции) Наблюдение и Исследовательский метод (Лабораторные работы)

1	2	3
защиту информации и сведений, составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз	иной охраняемой законом информации - меры, применяемые для обеспечения безопасности информации, комплексной защиты информации и сведений, составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз, способы организации и сопровождении аттестации и сертификации объекта информатизации по требованиям безопасности информации УМЕТЬ - реализовывать комплекс мер по обеспечению безопасности информации, комплексной защите информации и сведений, составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз, задавать, использовать профессионально-этические нормы в профессиональной деятельности в области информационной безопасности ВЛАДЕТЬ - навыками администрирования подсистемы информационной безопасности объекта информатизации, реализации комплекса мер по обеспечению безопасности информации, комплексной защиты информации и сведений, составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз	Метод проблемного обучения(Самостоятельная работа) **Активные и интерактивные методы обучения:** обсуждение практических примеров на лекциях
ОПКС-14 (10.05.03)	ЗНАТЬ - типовые модели угроз и модели нарушителей	**Формы обучения:** Фронтальная и групповая формы.

1	2	3
Способен осуществлять разработку, внедрение и эксплуатацию автоматизированной системы с учетом требований информационной безопасности и составлять технико-экономического обоснование проектных решений, включая подготовку исходных данных, и техническое задание на разработку системы защиты информации, а также способен выявлять недостатки существующих автоматизированных систем в соответствии с требованиями по защите информации	информационной безопасности	**Методы обучения:** Словесный метод обучения (Лекции) Наблюдение и Исследовательский метод (Лабораторные работы) Метод проблемного обучения(Самостоятельная работа) **Активные и интерактивные методы обучения:** обсуждение практических примеров на лекциях
ОПКС-16 (10.05.03) Способен исследовать современные проблемы информационной безопасности, анализировать процессы развития информационного общества, учитывая анализ основных этапов и закономерностей исторического развития России, ее место и роль в современном мире, в том числе для формирования гражданской позиции и развития патриотизма	ЗНАТЬ - содержание информационной безопасности как направления науки и области практической деятельности УМЕТЬ - использовать методы прикладной информатики для решения профессиональных задач - использовать методы и инструменты защиты информатики для исследования процесса развития информационного общества - учитывать различные контексты (социальные, культурные, национальные) патриотического и нравственного воспитания в сфере	**Формы обучения:** Фронтальная и групповая формы. **Методы обучения:** Словесный метод обучения (Лекции) Наблюдение и Исследовательский метод (Лабораторные работы) Метод проблемного обучения(Самостоятельная работа) **Активные и интерактивные методы обучения:** обсуждение практических примеров на лекциях

1	2	3
	профессиональной деятельности	
ОПКС-19 (10.05.03) Способен участвовать в разработке средств защиты информации подсистем обеспечения информационной безопасности в автоматизированных системах критически важных объектов	ЗНАТЬ - типовые модели угроз и модели нарушителей информационной безопасности	**Формы обучения:** Фронтальная и групповая формы. **Методы обучения:** Словесный метод обучения (Лекции) Наблюдение и Исследовательский метод (Лабораторные работы) Метод проблемного обучения(Самостоятельная работа) **Активные и интерактивные методы обучения:** обсуждение практических примеров на лекциях
ОПКС-20 (10.05.03) Способен организовать и обеспечить информационную безопасность при реализации технологических и бизнес-процессов организаций кредитно-финансовой сферы, в том числе процессов, связанных с осуществлением переводов денежных средств	ЗНАТЬ - угрозы безопасности информации, связанные с осуществлением переводов денежных средств УМЕТЬ - определять угрозы безопасности информации и разрабатывать модель угроз, модель нарушителя	**Формы обучения:** Фронтальная и групповая формы. **Методы обучения:** Словесный метод обучения (Лекции) Наблюдение и Исследовательский метод (Лабораторные работы) Метод проблемного обучения(Самостоятельная работа) **Активные и интерактивные методы обучения:** обсуждение практических примеров на лекциях
ОПКС-25 (10.05.03) Способен планировать и проводить анализ защищенности и верификацию программного обеспечения информационных систем	ЗНАТЬ - основные угрозы информационной безопасности объекта информатизации и их классификацию УМЕТЬ - определять угрозы защищенности компьютерных систем	**Формы обучения:** Фронтальная и групповая формы. **Методы обучения:** Словесный метод обучения (Лекции) Наблюдение и Исследовательский метод (Лабораторные работы) Метод проблемного обучения(Самостоятельная работа)

1	2	3
		Активные и интерактивные методы обучения: обсуждение практических примеров на лекциях
ОПКС-27 (10.05.03) Способен участвовать в проектировании системы управления информационной безопасностью автоматизированной системы в защищенном исполнении	ЗНАТЬ - типовые модели угроз и модели нарушителей информационной безопасности	**Формы обучения:** Фронтальная и групповая формы. **Методы обучения:** Словесный метод обучения (Лекции) Наблюдение и Исследовательский метод (Лабораторные работы) Метод проблемного обучения(Самостоятельная работа) **Активные и интерактивные методы обучения:** обсуждение практических примеров на лекциях
ПКС-6 (10.05.03/41 Анализ безопасности информационных систем) Способен участвовать в разработке требований по защите, формировании политик безопасности компьютерных систем и сетей	ЗНАТЬ - понятия угрозы, уязвимости, нарушителя информационной безопасности, рисков информационной безопасности, атаки, канала утечки информации, модели угроз, модели нарушителя, политики безопасности УМЕТЬ - проводить анализ угроз, уязвимостей, нарушителей и рисков информационной безопасности в компьютерных системах и сетях - составлять модель угроз в соответствии с требованиями нормативных документов	**Формы обучения:** Фронтальная и групповая формы. **Методы обучения:** Словесный метод обучения (Лекции) Наблюдение и Исследовательский метод (Лабораторные работы) Метод проблемного обучения(Самостоятельная работа) **Активные и интерактивные методы обучения:** обсуждение практических примеров на лекциях

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина входит в Блок Б1 «Дисциплины (модули)» образовательных программ специалитета по специальностям 10.05.03 «Информационная безопасность автоматизированных систем», 10.05.05 «Безопасность информационных технологий в правоохранительной сфере».

Изучение дисциплины предполагает предварительное освоение следующих дисциплин учебного плана:

- Теоретическая информатика
- Учебно-технологический практикум

Освоение учебной дисциплины связано с формированием компетенций с учетом матриц компетенций ОПОП для специальностей (уровень специалитета): 10.05.03 Информационная безопасность автоматизированных систем, 10.05.05 Безопасность информационных технологий в правоохранительной сфере.

3. ОБЪЕМ ДИСЦИПЛИНЫ

Общий объем дисциплины составляет 4 зачетные единицы (з.е.), которые состоят из 144 академических часа (ак.ч.) или 108 астрономических часов. В том числе: 1 семестр – 4 з.е. (144 ак.ч.).

Таблица 2. Объём дисциплины по видам учебных занятий (в ак.ч.)

Виды учебной работы	**Объем по семестрам, ак. ч.**	
	Всего	**Количество семестров освоения дисциплины**
		1
Объем дисциплины	144	144
Аудиторная работа*	**68**	**68**
Лекции (Л)	34	34
Лабораторные работы (ЛР)	34	34
Самостоятельная работа (СР)	**76**	**76**
Проработка учебного материала лекций	4.25	4.25
Подготовка к лабораторным работам	10	10
Подготовка к экзамену	30	30
Подготовка к контрольной работе	3	3
Выполнение домашнего задания	9	9
Другие виды самостоятельной работы	19.75	19.75
Вид промежуточной аттестации		**Экзамен**

*в том числе, в форме практической подготовки

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ, СТРУКТУРИРОВАННОЕ ПО МОДУЛЯМ УЧЕБНОЙ ДИСЦИПЛИНЫ С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ИЛИ АСТРОНОМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ

Таблица 3. Содержание дисциплины

№ п/п	Наименование модуля	Виды занятий*, ак.ч.				Шифр компетенций, закрепленных за модулем (код по СУОС 3++)	Текущий контроль		
		Л	С	ЛР	СР		Срок (неделя)	Контрольные мероприятия	Баллы (мин/ макс)
1 семестр									
1	Основные понятия и определения информационной безопасности	20	0	21	27	ОПКС-1, ОПКС-5, ОПКС-6, ОПКС-8, ОПКС-14, ОПКС-16, ОПКС-19, ОПКС-20, ОПКС-25, ОПКС-27, ПКС-6	10	Контрольная работа 1	5/9
								Интеракция на лекциях	7/10
								Лабораторный практикум	12/21
								ИТОГО:	**24/40**
2	Методы и средства обеспечения информационной безопасности	14	0	13	19	ОПКС-1, ОПКС-5, ОПКС-6, ОПКС-8, ОПКС-14, ОПКС-16, ОПКС-19, ОПКС-20, ОПКС-25, ОПКС-27, ПКС-6	17	Домашнее задание 1	5/9
								Интеракция на лекциях	5/7
								Лабораторный практикум	8/14
								ИТОГО:	**18/30**
3	Экзамен	-	-	-	30	ОПКС-1, ОПКС-5, ОПКС-6, ОПКС-8, ОПКС-14, ОПКС-16, ОПКС-19, ОПКС-20, ОПКС-25, ОПКС-27, ПКС-6	-	**Экзамен**	**18/30**
	ИТОГО за семестр	**34**	**0**	**34**	**76**	**-**	**-**	**-**	**60/100**

*в том числе, в форме практической подготовки

Содержание дисциплины, структурированное по темам (модулям)

№, п/п	Наименование модуля, содержание	Часы
1	**Основные понятия и определения информационной безопасности**	
	Лекции	20
1.1	Информационная безопасность в системе национальной безопасности РФ. Основные положения государственной информационной политики РФ	2
1.2	Понятие информационной безопасности. Ее составляющие	2
1.3	Угрозы информационной безопасности	2
1.4	Уязвимости информационной безопасности	2
1.5	Понятие нарушителя информационной безопасности	2
1.6	Атаки на информационную безопасность	2
1.7	Локальные атаки	2
1.8	Удаленные атаки	2
1.9	Атаки на потоки данных	2
1.10	Каналы утечки информации	2
	Лабораторные работы	21
ЛР1.1	Лабораторная работа №1. Выявление и оценка угроз информационной безопасности для объекта информатизации	7
ЛР1.2	Лабораторная работа №2. Сбор информации об уязвимостях объекта информатизации	7
ЛР1.3	Лабораторная работа №3. Разработка модели нарушителя для объекта информатизации	7
	Самостоятельная работа	27
СР1.1	Подготовка к контрольной работе №1	3
СР1.2	Проработка учебного материала лекций	2.5
СР1.3	Подготовка к лабораторным работам	6
СР1.4	Другие виды самостоятельной работы	15.5
2	**Методы и средства обеспечения информационной безопасности**	
	Лекции	14
2.1	Категории информации	2
2.2	Методы обеспечения информационной безопасности	4
2.3	Управление доступом к информации	8
	Лабораторные работы	13
ЛР2.1	Лабораторная работа №4. Сбор информации об атаках	7
ЛР2.2	Лабораторная работа №5. Реализация парольных методов доступа	6
	Самостоятельная работа	19
СР2.1	Выполнение домашнего задания №1	9
СР2.2	Проработка учебного материала лекций	1.75
СР2.3	Подготовка к лабораторным работам	4
СР2.4	Другие виды самостоятельной работы	4.25
3	**Экзамен**	**30**
СР3.1	Подготовка к экзамену	30

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Самостоятельная работа студентов по дисциплине обеспечивается следующими учебно-методическими материалами:

1. Рабочая программа дисциплины.
2. Перечень учебной литературы и дополнительных материалов, необходимых для освоения дисциплины [Раздел 7 Рабочей программы дисциплины].
3. Перечень ресурсов сети Интернет, рекомендуемых для самостоятельной работы при освоении дисциплины [Раздел 8 Рабочей программы дисциплины].
4. Методические указания для студентов по освоению дисциплины [Раздел 9 Рабочей программы дисциплины].
5. Перечень информационных технологий, используемых при изучении дисциплины, включая перечень программного обеспечения, информационных справочных систем и профессиональных баз данных [Раздел 10 Рабочей программы дисциплины].

Студенты получают доступ к указанным материалам начиная с первого занятия по дисциплине, в соответствии с ОПОП.

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ СТУДЕНТОВ ПО ДИСЦИПЛИНЕ

Фонд оценочных средств (ФОС) для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине базируется на перечне компетенций с указанием этапов их формирования в процессе освоения образовательной программы. ФОС обеспечивает объективный контроль достижения всех результатов обучения, запланированных для дисциплины.

ФОС включает в себя:

- перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы;
- описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания;
- типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения образовательной программы;
- методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Контроль освоения дисциплины производится в соответствии с Положением о текущем контроле успеваемости и промежуточной аттестации обучающихся в МГТУ им. Н.Э. Баумана.

7. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ И ДОПОЛНИТЕЛЬНЫХ МАТЕРИАЛОВ, НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Литература

1. Нестеров, С. А. Основы информационной безопасности : учебник для спо / С. А. Нестеров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 324 с. — ISBN 978-5-8114-9489-7.
2. Федоров, А. В. Политологические основы информационной безопасности : учебно-методическое пособие / А. В. Федоров. — Москва : МГТУ им. Н.Э. Баумана, 2019. — 36 с. — ISBN 978-5-7038-5253-8.
3. Нестеров, С. А. Основы информационной безопасности / С. А. Нестеров. — 3-е изд., стер. — Санкт-Петербург : Лань, 2024. — 324 с. — ISBN 978-5-507-49077-6.
4. Федоров А. В. Политологические основы информационной безопасности : учебно-методическое пособие / Федоров А. В. - Москва : МГТУ им. Н. Э. Баумана, 2019. - 32 с. - ISBN 978-5-7038-5253-8.
5. Федоров, А. В. Политологические основы информационной безопасности : учебное пособие / А. В. Федоров. — Москва : МГТУ им. Баумана, 2020. — 122 с. — ISBN 978-5-7038-5279-8.
6. Федоров А. В. Политологические основы информационной безопасности : учебное пособие / Федоров А. В. - Москва : МГТУ им. Н. Э. Баумана, 2020. - 122 с. - ISBN 978-5-7038-5279-8.
7. Федоров А. В. Политологические основы информационной безопасности : учебно-методическое пособие / Федоров А. В. ; МГТУ им. Н. Э. Баумана (национальный исследовательский ун-т). - М. : Изд-во МГТУ им. Н. Э. Баумана, 2019. - 32 с. - Библиогр.: с. 30-32. - ISBN 978-5-7038-5253-8.
8. Афонин А. И. Правовое обеспечение противодействия спамингу. Теоретические проблемы и решения / Афонин А. И. ; ред. Сычев М. П. - М. : Изд-во МГТУ им. Н. Э. Баумана, 2006. - 125 с. - Библиогр.: с. 117-124. - ISBN 5-7038-2864-3.

Дополнительные материалы

9. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения
10. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения
11. Доктрина информационной безопасности РФ
12. Стратегия национальной безопасности РФ
13. Методический документ ФСТЭК «Методика оценки угроз безопасности информации»
14. Методический документ ФСТЭК «Руководство по управлению уязвимостями»
15. Методический документ ФСТЭК «Методика оценки критичности уязвимостей»
16. Методический документ ФСТЭК «Методика тестирования обновлений»

8. ПЕРЕЧЕНЬ РЕСУРСОВ СЕТИ ИНТЕРНЕТ, РЕКОМЕНДУЕМЫХ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПРИ ОСВОЕНИИ ДИСЦИПЛИНЫ

1. Сайт университета: http://bmstu.ru
2. Электронная образовательная среда МФ МГТУ им. Н.Э.Баумана http://portaldo.mgul.ac.ru/
3. Библиотека МГТУ им. Н.Э. Баумана http://library.bmstu.ru.
4. Сайт Издательства МГТУ им. Н.Э. Баумана https://press.bmstu.ru
5. Научно-техническая библиотека КФ МГТУ им. Н.Э. Баумана. http://library.bmstu-kaluga.ru.
6. Библиотека МФ МГТУ им. Н. Э. Баумана https://mf.bmstu.ru/info/library/
7. Российская государственная библиотека http://www.rsl.ru.
8. Государственная публичная научно-техническая библиотека России http://www.gpntb.ru.
9. Научная электронная библиотека http://eLIBRARY.RU.
10. Электронно-библиотечная система издательства «Лань» http://e.lanbook.com.
11. Электронно-библиотечная система «Университетская библиотека онлайн» http://biblioclub.ru.
12. Электронно-библиотечная система «IPRbooks» http://www.iprbookshop.ru.
13. Электронно-библиотечная система (ЭБС) «Юрайт» https://biblio-online.ru.
14. Центральная библиотека образовательных ресурсов Минобрнауки РФ www.edulib.ru.
15. Единая коллекция цифровых образовательных ресурсов http://school-collection.edu.ru.
16. Федеральный центр информационно-образовательных ресурсов http://fcior.edu.ru.
17. Электронно-библиотечная система https://ibooks.ru/.
18. Виртуальный читальный зал РГБ https://ldiss.rsl.ru/.
19. Национальная Электронная Библиотека (НЭБ) https://rusneb.ru/.
20. Электронно-библиотечная система, которая содержит электронные версии учебников, учебных и научных пособий, монографий по различным областям знаний https://book.ru/.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ СТУДЕНТОВ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Приступая к работе, каждый студент должен принимать во внимание нижеследующие положения.

Дисциплина построена по модульному принципу, каждый модуль представляет собой логически завершенный раздел дисциплины. Дисциплина делится на три модуля (включая экзамен).

На первом занятии студент получает информацию для доступа к комплексу методических материалов по дисциплине.

Лекции посвящены рассмотрению ключевых, базовых положений дисциплины и разъяснению учебных заданий, выносимых на самостоятельную проработку.

Практическая подготовка может включать в себя отдельные занятия лекционного типа, которые предусматривают передачу учебной информации обучающимся, необходимой для последующего выполнения работ, связанных с будущей профессиональной деятельностью.

Лабораторные работы предназначены для приобретения опыта практической реализации основной профессиональной образовательной программы. Методические документы к лабораторным работам прорабатываются студентами во время занятий и самостоятельной работы. Необходимый уровень подготовки контролируется перед проведением лабораторных работ.

Практическая подготовка при реализации учебной дисциплины организуется путем проведения семинаров, практикумов, лабораторных работ и индивидуальных и(или) групповых консультаций, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

Самостоятельная работа студентов включает следующие виды: проработка учебного материала лекций, подготовка к лабораторным работам, подготовка к экзамену, подготовка к контрольной работе, выполнение домашнего задания. Результаты всех видов работы студентов формируются в виде личного рейтинга, который учитывается на промежуточной аттестации. Самостоятельная работа предусматривает не только проработку материалов лекций, но и их расширение в результате поиска, анализа, структурирования и представления в компактном виде современной информации из всех возможных источников.

Текущий контроль проводится в течение каждого модуля, его результаты складываются из оценок по следующим видам контрольных мероприятий:

- Контрольная работа
- Домашнее задание.

Освоение дисциплины и ее успешное завершение на стадии промежуточной аттестации возможно только при регулярной работе во время семестра и планомерном прохождении текущего контроля.

Для завершения работы в семестре студент должен выполнить все контрольные мероприятия, входящие в текущий контроль.

Контрольное мероприятие считается выполненным, если за него студент получил оценку в баллах, не ниже минимальной оценки, установленной программой дисциплины по данному мероприятию.

Студенты, не сдавшие контрольное мероприятие в установленный срок, продолжают работать над ним в соответствие с порядком, принятым кафедрой.

Промежуточная аттестация по дисциплине проходит в форме экзамена, контролирующего освоение ключевых, базовых положений дисциплины, составляющих основу остаточных знаний по ней.

Методика оценки по рейтингу

Студент, выполнивший все предусмотренные учебным планом задания и сдавший все контрольные мероприятия, получает итоговую оценку по дисциплине за семестр в соответствии со шкалой:

Рейтинг	**Оценка на экзамене**
85 – 100	отлично
71 – 84	хорошо
60 – 70	удовлетворительно
0 – 59	неудовлетворительно

Оценивание дисциплины ведется в соответствии с Положением о текущем контроле успеваемости и промежуточной аттестации обучающихся в МГТУ им. Н.Э. Баумана.

10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ИЗУЧЕНИИ ДИСЦИПЛИНЫ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ И ПРОФЕССИОНАЛЬНЫХ БАЗ ДАННЫХ

Информационные технологии:

– Электронная информационно-образовательная среда МГТУ им. Н.Э. Баумана обеспечивает доступ к учебным планам, рабочим программам дисциплин (модулей), программам практик, электронным учебным изданиям и электронным образовательным ресурсам, указанным в рабочих программах дисциплин (модулей), программах практик, формирование электронного портфолио обучающегося, в том числе сохранение его работ и оценок за эти работы. Предусмотрена возможность синхронного и асинхронного взаимодействия студентов и преподавателей посредством технологий и служб по пересылке и получению электронных сообщений между пользователями компьютерной сети Интернет.
– Электронная почта преподавателя: lachikhinaab@bmstu.ru;
– Система BigBlueButton https://webinar.bmstu.ru;
– Электронная образовательная система МГТУ им. Н.Э.Баумана https://e-learning.bmstu.ru/

Программное обеспечение:

– LibreOffice
– Альт Образование

Информационные справочные системы:

– Информационно-правовая система «Гарант» http://www.garant.ru;
– Информационно-правовая система «Консультант Плюс» http://www.consultant.ru;
– Библиотека нормативных технических документов в сфере навигации и применения ГЛОНАСС https://glonassunion.ru/regulatory-control/technical;
– Каталог национальных стандартов (Росстандарт) https://www.rst.gov.ru/portal/gost;
– Портал корпорации «Роскосмос» http://www.roscosmos.ru/;
– Научно-образовательный портал «Большая российская энциклопедия» https://bigenc.ru;

Профессиональные базы данных:

– Портал машиностроения http://www.mashportal.ru;
– Единая база ГОСТов РФ https://gostexpert.ru;
– Электронный фонд правовой и нормативно-технической информации https://docs.cntd.ru;
– Государственная статистика РФ http://fedstat.ru;
– БДУ ФСТЭК России https://bdu.fstec.ru

11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Перечень материально-технического обеспечения дисциплины

№, п/п	Вид занятий	Вид и наименование оборудования
1	Лекции	специально оборудованные аудитории с мультимедийными средствами, средствами звуковоспроизведения и имеющими выход в сеть Интернет; помещения для проведения аудиторных занятий, оборудованные учебной мебелью; аудитории оснащенные компьютерами с доступом к базам данных и сети Интернет; студии; компьютерные классы.
2	Лабораторные работы	специально оборудованные аудитории с мультимедийными средствами, средствами звуковоспроизведения и имеющими выход в сеть Интернет; помещения для проведения аудиторных занятий, оборудованные учебной мебелью; аудитории оснащенные компьютерами с доступом к базам данных и сети Интернет; студии; компьютерные классы.
3	Самостоятельная работа	библиотека, имеющая рабочие места для студентов; выставочные залы; аудитории, оснащенные компьютерами с доступом к сети Интернет. Социокультурное пространство университета позволяет студенту качественно выполнять самостоятельную работу.