Министерство науки и высшего образования Российской Федерации
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)

Заместитель директора
по учебной работе
КФ МГТУ им. Н.Э. Баумана
_____ О.Л. Перерва
«13» мая 2022 г.

Факультет ИУК «Информатика и управление»

Кафедра ИУК6 «Защита информации»

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

Преддипломная практика

Автор программы:
Твердова С.М., доцент (к.н.), кандидат технических наук, доцент, tverdovasm@bmstu.ru

Утверждена на заседании кафедры «Защита информации»
Протокол № 9 заседания кафедры «ИУК6» от 07.04.2022 г.

Заместитель председателя Методической комиссии
КФ МГТУ им. Н.Э. Баумана
Малышев Е.Н. _____

Рабочая программа одобрена на 2023/2024 учебный год.
Протокол № 32.00-80-05/4 заседания кафедры «ИУК6» от 06.04.2023 г.
Лист переутверждения рабочей программы дисциплины / практики.

Рабочая программа одобрена на 2024/2025 учебный год.
Протокол № 07.04.06-04.08/4 заседания кафедры «ИУК6» от 04.04.2024 г.
Лист переутверждения рабочей программы дисциплины / практики.

ОГЛАВЛЕНИЕ

с.

1. ВИД ПРАКТИКИ, СПОСОБ И ФОРМЫ ЕЕ ПРОВЕДЕНИЯ

1.1 Вид практики – Производственная практика.
1.2. Способы проведения практики – стационарная и (или) выездная.
1.3. Форма проведения практики – практика проводится в форме практической подготовки;
– непрерывно;
1.4. Тип практики – Преддипломная практика.

2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПРИ ПРОХОЖДЕНИИ ПРАКТИКИ, СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Настоящая программа практики устанавливает планируемые результаты практики, а также определяет содержание практики и отчетности.

Программа разработана в соответствии с основными профессиональными образовательными программами (ОПОП) и учебными планами КФ МГТУ им. Н.Э. Баумана, составленными на основе самостоятельно устанавливаемых образовательных стандартов (СУОС 3++):

для специальности (уровень специалитета): 10.05.03 «Информационная безопасность автоматизированных систем».

Освоение дисциплины вносит вклад в формирование компетенций, предусмотренных ОПОП:

Код компетенции по СУОС 3++	**Формулировка компетенции**
	Универсальные компетенции собственные
УКС-2 (10.05.03)	Способен управлять проектом на всех этапах его жизненного цикла, самостоятельно выбирая способы решения проблем, использовать основы экономических и правовых знаний для оценки эффективности результатов профессиональной деятельности
	Профессиональные компетенции собственные (обязательные)
ПКСо-1 (10.05.03)	Способен разрабатывать проектные решения по защите информации в автоматизированных системах
ПКСо-2 (10.05.03)	Способен разрабатывать рабочую документацию на систему защиты информации автоматизированных систем
	Профессиональные компетенции собственные
ПКС-3 (10.05.03/41 Анализ безопасности информационных систем)	Способен осуществлять тестирование систем защиты информации автоматизированных систем
ПКС-4 (10.05.03/41 Анализ безопасности информационных систем)	Способен участвовать в разработке программных и программно-аппаратных средств для систем защиты информации автоматизированных систем
ПКС-5 (10.05.03/41 Анализ	Способен участвовать в проведении контрольных проверок работоспособности и эффективности применяемых программно – аппаратных средств защиты информации

безопасности информационных систем)	
ПКС-6 (10.05.03/41 Анализ безопасности информационных систем)	Способен участвовать в разработке требований по защите, формировании политик безопасности компьютерных систем и сетей
ПКС-7 (10.05.03/41 Анализ безопасности информационных систем)	Способен участвовать в проведении анализа безопасности компьютерных систем
ПКС-8 (10.05.03/41 Анализ безопасности информационных систем)	Способен участвовать в проведении инструментального мониторинга защищенности компьютерных систем и сетей

Для категорий «знать, уметь, владеть» планируется достижение результатов обучения (РО), вносящих на соответствующих уровнях вклад в формирование компетенций, предусмотренных основной профессиональной образовательной программой (табл. 1).

Таблица 1. Индикаторы достижения компетенции

1	2	3
Компетенция: код по СУОС 3++, формулировка	**Индикаторы достижения компетенции**	**Формы и методы обучения, способствующие формированию и развитию компетенции**
УКС-2 (10.05.03) Способен управлять проектом на всех этапах его жизненного цикла, самостоятельно выбирая способы решения проблем, использовать основы экономических и правовых знаний для оценки эффективности результатов профессиональной деятельности	ЗНАЕТ: - этапы жизненного цикла проекта, его разработки и реализации - методы разработки и управления проектами - действующее законодательство и правовые нормы, регулирующие профессиональную деятельность; УМЕЕТ: - разрабатывать, определять целевые этапы, основные направления работ - управлять проектом на всех этапах его жизненного цикла, в том числе в нестандартных ситуациях - использовать нормативно-правовую документацию в сфере профессиональной деятельности; ВЛАДЕЕТ: - методиками разработки и управления проектом - методами оценки потребности в ресурсах и эффективности проекта	**Контактная работа во взаимодействии студентов с руководителями практики от Университета и от предприятия** Активные и интерактивные методы обучения **Самостоятельная работа** Практическая подготовка

1	2	3
ПКСо-1 (10.05.03) Способен разрабатывать проектные решения по защите информации в автоматизированных системах	ЗНАЕТ: - методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и систем защиты информации автоматизированных системах - основные средства, способы и принципы построения систем защиты информации автоматизированных систем; УМЕЕТ: - проводить технико-экономическое обоснование проектных решений средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защищенности - исследовать эффективность проектных решений средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защищенности; ВЛАДЕЕТ: - навыками анализа защищенности информационной инфраструктуры автоматизированной системы	**Контактная работа во взаимодействии студентов с руководителями практики от Университета и от предприятия** Активные и интерактивные методы обучения **Самостоятельная работа** Практическая подготовка
ПКСо-2 (10.05.03) Способен разрабатывать рабочую документацию на систему защиты информации автоматизированных систем	ЗНАЕТ: - последовательность и содержание этапов разработки автоматизированных систем и систем защиты информации автоматизированных системах - национальные стандарты в области создания автоматизированных систем; УМЕЕТ: - разрабатывать технические задания на создание систем информационной безопасности автоматизированных систем - составлять документацию для проектных решений средств обеспечения защиты информации в автоматизированной системе по обеспечению требуемого уровня защищенности; ВЛАДЕЕТ: - навыками анализа технической документации информационной инфраструктуры автоматизированной системы	**Контактная работа во взаимодействии студентов с руководителями практики от Университета и от предприятия** Активные и интерактивные методы обучения **Самостоятельная работа** Практическая подготовка

1	2	3
ПКС-3 (10.05.03/41 Анализ безопасности информационных систем) Способен осуществлять тестирование систем защиты информации автоматизированных систем	ЗНАЕТ: - средства тестирования системы защиты информации автоматизированных систем - методики тестирования и оценивания систем защиты информации автоматизированных систем - характеристики и показатели, подлежащие тестированию в системах защиты информации автоматизированных систем; УМЕЕТ: - составлять план тестирования системы защиты информации автоматизированных систем - применять методы и средства тестирования системы защиты информации автоматизированных систем - определять характеристики и показатели, подлежащие тестированию в системе защиты информации автоматизированных систем в конкретном случае - проводить анализ полученных результатов тестирования системы защиты информации автоматизированной системы - оформлять результаты тестирования с использованием пакетов прикладных программ; ВЛАДЕЕТ: - навыками планирования и проведения тестирования систем защиты информации автоматизированных систем - навыками анализа и оценивания полученных результатов тестирования систем защиты информации автоматизированных систем - навыками формирования отчета о проведенном тестировании системы защиты информации автоматизированных систем	**Контактная работа во взаимодействии студентов с руководителями практики от Университета и от предприятия** Активные и интерактивные методы обучения **Самостоятельная работа** Практическая подготовка
ПКС-4 (10.05.03/41 Анализ безопасности информационных систем) Способен участвовать в разработке программных и программно-аппаратных	ЗНАЕТ: - технологии разработки программных и программно-аппаратных средств; - особенности разработки средств для систем защиты информации; - языки программирования высокого и низкого уровней, различные виды компиляторов;	**Контактная работа во взаимодействии студентов с руководителями практики от Университета и от предприятия** Активные и интерактивные методы обучения **Самостоятельная работа** Практическая подготовка

1	2	3
средств для систем защиты информации автоматизированных систем	- основы электроники и схемотехники; - современную элементную базу; УМЕЕТ: - разрабатывать алгоритмы; - разрабатывать архитектуру аппаратных средств в составе программно – аппаратных комплексов; - применять современные среды разработки и отладки программных средств, среды разработки и эмуляции программно – аппаратных для систем защиты информации автоматизированных систем; - разрабатывать проектную и эксплуатационную документацию в соответствии с ГОСТ; - составлять план тестирования программных и программно – аппаратных средств; ВЛАДЕЕТ: - навыками разработки программных и программно – аппаратных средств защиты информации; - приемами безопасной разработки программных и аппаратных продуктов, в том числе с применением механизмов защиты от несанкционированного доступа; - навыками разработки комплекта документации на разработанные средства; - навыками проведения тестирования и внедрения разработанных продуктов; - навыками оптимизации программной составляющей программно – аппаратных комплексов защиты информации	
ПКС-5 (10.05.03/41 Анализ безопасности информационных систем) Способен участвовать в проведении контрольных проверок работоспособности и эффективности применяемых программно – аппаратных средств защиты информации	ЗНАЕТ: - методики проведения проверок работоспособности и эффективности применяемых программно – аппаратных средств защиты информации - понятия контрольной проверки, работоспособности, эффективности - критерии оценки эффективности применяемых программно-аппаратных средств защиты информации	**Контактная работа во взаимодействии студентов с руководителями практики от Университета и от предприятия** Активные и интерактивные методы обучения **Самостоятельная работа** Практическая подготовка

1	2	3
	- критерии оценки работоспособности применяемых программно-аппаратных средств защиты информации; УМЕЕТ: - составлять отчеты по результатам проверок - проводить анализ полученных при проведении контрольных проверок результатов - составлять план проведения контрольных проверок - выбирать пороговые значения критериев оценки работоспособности применяемых программно-аппаратных средств защиты информации; ВЛАДЕЕТ: - навыками проведения контрольных проверок работоспособности и эффективности применяемых программно – аппаратных средств защиты информации	
ПКС-6 (10.05.03/41 Анализ безопасности информационных систем) Способен участвовать в разработке требований по защите, формировании политик безопасности компьютерных систем и сетей	ЗНАЕТ: - нормативно – правовую базу защиты информации в компьютерных системах и сетях - понятия угрозы, уязвимости, нарушителя информационной безопасности, рисков информационной безопасности, атаки, канала утечки информации, модели угроз, модели нарушителя, политики безопасности - методику обследования защищенности компьютерных систем и сетей - методику формирования политики безопасности; УМЕЕТ: - проводить анализ угроз, уязвимостей, нарушителей и рисков информационной безопасности в компьютерных системах и сетях - составлять модель угроз в соответствии с требованиями нормативных документов - технически грамотным языком излагать требования по защите информации; ВЛАДЕЕТ:	**Контактная работа во взаимодействии студентов с руководителями практики от Университета и от предприятия** Активные и интерактивные методы обучения **Самостоятельная работа** Практическая подготовка

1	2	3
	- навыками разработки требований по защите компьютерных систем и сетей - навыками формирования политик безопасности компьютерных систем и сетей	
ПКС-7 (10.05.03/41 Анализ безопасности информационных систем) Способен участвовать в проведении анализа безопасности компьютерных систем	ЗНАЕТ - нормативно – правовую базу защиты информации в компьютерных системах - основные понятия в области анализа безопасности компьютерных систем - методики анализа безопасности компьютерных систем - методы и средства обеспечения безопасности компьютерных систем УМЕЕТ - определять наименее защищенные узлы компьютерных систем - проводить анализ угроз, уязвимостей, нарушителей и рисков информационной безопасности в автоматизированных системах - подбирать и применять методы, средства, критерии и инструменты для проведения анализа безопасности компьютерных систем - использовать реестры общеизвестных уязвимостей - разрабатывать рекомендации по устранению уязвимостей автоматизированных систем и обеспечению их безопасного функционирования ВЛАДЕЕТ - навыками анализа безопасности компьютерных систем - навыками администрирования средств обеспечения безопасности компьютерных систем	**Контактная работа во взаимодействии студентов с руководителями практики от Университета и от предприятия** Активные и интерактивные методы обучения **Самостоятельная работа** Практическая подготовка
ПКС-8 (10.05.03/41 Анализ безопасности информационных систем) Способен участвовать в проведении инструментального мониторинга защищенности компьютерных систем и сетей	ЗНАЕТ - нормативно – правовую базу защиты информации в компьютерных системах и сетях - средства инструментального мониторинга защищенности - механизмы и алгоритмы проведения мониторинга защищенности отдельных сегментов, сервисов и узлов компьютерных систем и сетей	**Контактная работа во взаимодействии студентов с руководителями практики от Университета и от предприятия** Активные и интерактивные методы обучения **Самостоятельная работа** Практическая подготовка

1	2	3
	- алгоритмы поиска неисследованных уязвимостей и недокументированных возможностей аппаратных и программных средств УМЕЕТ - составлять план проведения инструментального мониторинга защищенности для заданной компьютерной системы или сети - подбирать средства инструментального мониторинга защищенности для заданной компьютерной системы или сети - собирать статистические сведения о работе компьютерных систем и сетей в ручном и автоматизированном режиме, анализировать полученные данные, выдавать заключение о защищенности компьютерных систем и сетей - применять различные механизмы и алгоритмы поиска уязвимостей сетевых сервисов и компьютерных систем - проводить исследовательский поиск необнаруженных ранее уязвимостей и недокументированных возможностей ВЛАДЕЕТ - навыками проведении инструментального мониторинга защищенности компьютерных систем и сетей	

3. МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Практика входит в Блок 2. «Практика» образовательной программы и относится к обязательной части.

Участие студента в формировании своей образовательной программы при прохождении практики заключается в следующем:

- студент имеет право предложить в качестве базы практики предприятие, где он предполагает осуществлять свою профессиональную деятельность по завершению обучения или представляющее лично для него наибольший профессиональный интерес и имеющий наибольшую значимость для выпускной квалификационной работы;
- при формировании индивидуального задания студент имеет право предложить для самостоятельного изучения объект (процесс), представляющий лично для него наибольший профессиональный интерес и имеющий наибольшую значимость для выпускной квалификационной работы.

4. ОБЪЕМ ПРАКТИКИ

Количество семестров прохождения практики: 1.

Общий объем практики составляет 20 зачетных единицы (з.е.), 720 академических часов (540 астрономических часов). В том числе: в 1-ом семестре – 20 з.е (720 ак.ч.).

Таблица 2. Объём практики по видам учебных занятий (в академических часах)

Виды учебной работы	**Всего**	**Объем по семестрам**
		1
Практика	720	720
Вид промежуточной аттестации		**ДЗачёт**

5. СОДЕРЖАНИЕ ПРАКТИКИ

№ пп	Этапы практики	Час.
	1 семестр	720
5.1	Научно-исследовательская часть	150-198
5.2	Проектно-конструкторская часть	150-200
5.3	Контрольно-аналитическая часть	150-200
5.4	Организационно-управленческая часть	100-120
5.5	Промежуточная аттестация	2

Содержание

Научно-исследовательская часть

Задачи:

подготовить материалы для выполнения раздела ВКР, ориентированного на решение полностью или частично следующих задач профессиональной деятельности:

– Разработка проектных решений по защите информации в автоматизированных системах.

Проектно-конструкторская часть

Задачи:

подготовить материалы для выполнения раздела ВКР, ориентированного на решение полностью или частично следующих задач профессиональной деятельности:

– Разработка программных и программно-аппаратных средств для систем защиты информации автоматизированных систем.

Контрольно - аналитическая часть

Задачи:

подготовить материалы для выполнения раздела ВКР, ориентированного на решение полностью или частично следующих задач профессиональной деятельности:

– Тестирование систем защиты информации автоматизированных систем;

– Проведение контрольных проверок работоспособности и эффективности применяемых программно – аппаратных средств защиты информации;

– Проведение анализа безопасности компьютерных систем;

– Проведение инструментального мониторинга защищенности компьютерных систем и сетей.

Организационно-управленческая часть

Задачи:
подготовить материалы для выполнения раздела ВКР, ориентированного на решение полностью или частично следующих задач профессиональной деятельности:
– Разработка эксплуатационной документации на системы защиты информации автоматизированных систем;
– Разработка требований по защите, формирование политик безопасности компьютерных систем и сетей.

Промежуточная аттестация

Промежуточная аттестация проводится с учетом своевременности выполнения заданий, качества выполнения заданий и защиты полученных результатов.

6. ФОРМА ОТЧЕТНОСТИ ПО ПРАКТИКЕ

Преддипломная практика проводится для сбора и анализа материалов для выполнения выпускной квалификационной работы.

Форма отчетности по практике – письменный отчет.

Форма промежуточной аттестации по практике – зачет с выставлением дифференцированной оценки.

Структура отчета студента по практике:
- Титульный лист. На титульном листе указывается официальное название МГТУ им. Н.Э. Баумана, факультета, выпускающей кафедры, ФИО студента, группа, название практики, должности и ФИО руководителя практики.
- Содержание (оглавление).
- Введение. В разделе должны быть приведены задачи практики.
- Основная часть. В разделе приводится описание выполненных студентом работ в соответствии с задачами практики и индивидуальным заданием, приводятся полученные студентом результаты моделирования и проектирования.
- Заключение. В разделе должны быть представлены выводы по результатам практики.
- Список использованных источников.
- Приложения (при необходимости).

Сброшюрованный отчет подписывается руководителем практики.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Самостоятельная работа студентов обеспечивается следующими учебно-методическими материалами:
1. Программа практики.
2. Учебная литература и дополнительные материалы [Раздел 9 Программы практики].
3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» [Раздел 10 Программы практики].
4. Методические указания для обучающихся по практике [Раздел 11 Программы практики], обеспечивающие самостоятельную работу студента.
5. Комплект индивидуальных заданий.

Студенты начинают получать доступ к указанным материалам накануне начала практики.

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ СТУДЕНТОВ ПО ПРАКТИКЕ

Фонд оценочных средств (ФОС) для проведения текущего контроля и промежуточной аттестации обучающихся по практике базируется на перечне компетенций с указанием

этапов их формирования в процессе освоения образовательной программы (раздел 1). ФОС обеспечивает объективный контроль достижения всех результатов обучения, запланированных для практики.

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, владений и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения образовательной программы;
- методические материалы, определяющие процедуры оценивания знаний, умений, владений и (или) опыта деятельности, характеризующих этапы формирования компетенций.

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

ФОС является приложением к данной программе практики.

Промежуточная аттестация

Формой промежуточной аттестации по практике является дифференцированный зачёт.

Суммарное количество баллов, начисленных студенту по итогам выполнения им всех видов учебной работы и контрольных мероприятий, предусмотренных программой практики, представляет собой балльную оценку по практике в ходе промежуточной аттестации. Перевод балльной оценки в дифференцированную оценку осуществляется в соответствии с таблицей.

Балльная оценка по практике	**Дифференцированная оценка результатов промежуточной аттестации**
90 – 100	Отлично
75 – 89	Хорошо
60 – 74	Удовлетворительно
0-59	Неудовлетворительно

9. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ И ДОПОЛНИТЕЛЬНЫХ МАТЕРИАЛОВ, НЕОБХОДИМЫХ ДЛЯ ПРОВЕДЕНИЕ ПРАТИКИ

Литература по практике

1. Вылегжанина, А.О. Разработка проекта : учеб. пособие / А.О. Вы-легжанина. - М.; Берлин: Директ-Медиа, 2015. - 291 с. – URL: http://biblioclub.ru/index.php?page=book&id=275277.
2. Ласковец, С.В. Методология научного творчества : учеб. пособие / С.В. Ласковец. - М.: Евразийский открытый институт, 2010. - 32 с. – URL: http://biblioclub.ru/index.php?page=book&id=90384.
3. Основы научного творчества Учебное пособие / Аверченков В.И., Малахов Ю.А. - 2012. - URL: http://www.iprbookshop.ru/7004.html.
4. Тумбинская, М. В. Защита информации на предприятии: учебное пособие / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург: Лань, 2020. — 184 с. — ISBN 978-5-8114-

4291-1. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/130184.
5. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю. Н. Загинайлов. – М.-Берлин: Изд-во «Директ-Медиа», 2015. – 253 с. – URL: http://biblioclub.ru/index.php?page=book&id=276557
6. Васильков, А.В. Информационные системы и их безопасность [Текст] / А.В. Васильков, А.А. Васильков, И.А. Васильков. – М.: Изд-во «Форум», 2013. – 528 с.
7. Денисов, В.В. Анализ состояния защиты данных в информационных системах: учебно-методическое пособие / В.В. Денисов. – Новосибирск: Изд-во НГТУ, 2012. – 52 с. – URL: http://biblioclub.ru/index.php?page=book&id=228844
8. Кияев, В.И., Граничин, О.Н. Безопасность информационных систем : курс лекций / В.И. Кияев, О.Н. Граничин. - М.: Национальный Открытый Университет «ИНТУИТ», 2016. - 192 с. – URL: https://biblioclub.ru/index.php?page=book_red&id=429032.
9. Фридман, А. Л. Язык программирования Си++ : [16+] / А. Л. Фридман. – 2-е изд., исправ. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 219 с. – (Основы информационных технологий). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=578114
10. Царев, Р.Ю. Программирование на языке Си : учебное пособие / Р.Ю. Царев. – Красноярск: Сибирский федеральный университет, 2014. – 108 с.: табл., схем – URL: http://biblioclub.ru/index.php?page=book&id=364601
11. Имитационное моделирование Учебное пособие. - 2019. - URL: http://www.iprbookshop.ru/101442.html.
12. Душкин, А.В., Ланкин, О.В., Потехецкий, С.В., Данилкин, А.П., Малышев, А.А. Методологические основы построения защищенных автоматизированных систем [Электронный ресурс]: учебное пособие / А.В. Душкин, О.В. Ланкин, С.В, Потехецкий [и др.] – Воронеж: ВГУИТ, 2013. – 258 с. – Режим доступа: https://biblioclub.ru/index.php?page=book_view_red&book_id=255851 .
13. Пелешенко, В.С., Говорова, С.В., Лапина, М.А. Менеджмент инцидентов безопасности защищенных автоматизированных систем управления: учебное пособие / В.С. Пелешенко, С.В. Говорова, М.А. Лапина. – Ставрополь: Изд-во СКФУ, 2017. – 86 с.: ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=467139
14. Коробова, И.Л. Принятие решений в системах, основанных на знаниях [Электронный ресурс]: учеб. пособие / И.Л. Коробова, Г.В. Артемов – Тамбов: Издательство ФГБОУ ВПО «ТГТУ», 2012. – 81 с. – URL: http://biblioclub.ru/index.php?page=book_red&id=277800&sr=1
15. Говорова, С.В., Пелешенко, В. С. Основы управленческой деятельности: учеб. пособие / С.В. Говорова, В.С. Пелешенко. – Ставрополь: СКФУ, 2016. – 109 с. - URL: https://biblioclub.ru/index.php?page=book_view_red&book_id=457963.
16. Учитель, Ю.Г., Терновой, А.И., Терновой, К.И. Разработка управленческих решений: учебник / Ю.Г. Учитель, А.И. Терновой, К.И. Терновой. – М.: Юнити-Дана, 2015. – 383 с. URL: https://biblioclub.ru/index.php?page=book_view_red&book_id=117136.

Дополнительные материалы

18. ГОСТ 2.105-79. ЕСКД. Общие требования к текстовым документам.
ГОСТ 7.32-2017 Система стандартов по информации, библиотечному и издательскому делу. Отчет о научно-исследовательской работе. Структура и правила оформления.
19. ГОСТ Р ИСО 9001-2008 Системы менеджмента качества. Требования.
20. ГОСТ Р 53603-2009. Оценка соответствия. Схемы сертификации продукции в Российской Федерации.
21. ГОСТ Р 7.0.5-2008 Система стандартов по информации, библиотечному и издательскому делу. Библиографическая ссылка. Общие требования и правила составления.
22. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 N 149-ФЗ.

23. Федеральный закон "О связи" от 07.07.2003 N 126-ФЗ.
24. Федеральный закон "О безопасности" от 28.12.2010 N 390-ФЗ
25. Федеральный закон "Об электронной подписи" от 06.04.2011 N 63-ФЗ.
26. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ.
27. Федеральный закон "О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных" от 19.12.2005 N 160-ФЗ.
28. Федеральный закон "О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием федерального закона "О ратификации Конвенции Совета Европы О защите физических лиц при автоматизированной обработке персональных данных" и федерального закона "О персональных данных" от 7.05.2013 N 99-ФЗ.
29. Федеральный закон "О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях" от 21.07.2014 N 242-ФЗ.
30. Закон РФ "О государственной тайне" от 21.07.1993 N 5485-1.
31. Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ.
32. Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ.
33. Федеральный закон "О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 193-ФЗ.
33. Федеральный закон "О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 194-ФЗ.
34. Федеральный закон "О банках и банковской деятельности" от 02.12.1990 N 395-1.
35. Федеральный закон "О лицензировании отдельных видов деятельности" от 04.05.2011 N 99-ФЗ.
36. Федеральный закон "Об экспортном контроле" от 18.07.1999 г. N 183-ФЗ .
37. Федеральный закон "О техническом регулировании" от 27.12.2002 N 184-ФЗ.
38. Трудовой кодекс Российской Федерации от 30.12.2001 N 197-ФЗ.
39. Гражданский кодекс Российской Федерации часть 4 (ГК РФ ч.4) 18.12.2006 N 230-ФЗ.
40. "Кодекс Российской Федерации об административных правонарушениях" от 30.12.2001 N 195-ФЗ.
41. "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ.
42. Доктрина информационной безопасности Российской Федерации.
43. Методика оценки угроз безопасности информации. Методический документ ФСТЭК России 5 февраля 2021 г.
44. Меры защиты информации в государственных информационных системах. Методический документ ФСТЭК России 11 февраля 2014 г.
45. ГОСТ Р 51897-2002 Менеджмент риска. Термины и определения
46. ГОСТ Р ИСО 31000-2010 МЕНЕДЖМЕНТ РИСКА. ПРИНЦИПЫ И РУКОВОДСТВО
47. ГОСТ Р ИСО/МЭК 31010-2011 МЕНЕДЖМЕНТ РИСКА. МЕТОДЫ ОЦЕНКИ РИСКА
48. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
49. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
50. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения
51. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения
52. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения
53. ГОСТ Р 56939-2016 Защита информации. Разработка безопасного программного обеспечения. Общие требования.

54. ОСТ Р ИСО/МЭК 27001-2006 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.
55. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.
56. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.
57. ГОСТ Р ИСО/МЭК 27003-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности.
58. ГОСТ Р ИСО/МЭК 27004-2011 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения.
59. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.
60. ГОСТ Р ИСО/МЭК 27006-2008 Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности.
61. ГОСТ Р ИСО/МЭК 27013-2014 Информационная технология. Методы и средства обеспечения безопасности. Руководство по совместному использованию стандартов ИСО/МЭК 27001 и ИСО/МЭК 20000-1.
62. ГОСТ Р ИСО/МЭК 27033-1-2014 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции
63. ГОСТ Р ИСО/МЭК 27033-2-2014 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 2. Рекомендации по проектированию и реализации безопасности сети
64. ГОСТ Р ИСО/МЭК 27033-3-2014 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления
65. ГОСТ Р ИСО/МЭК 27033-4-2014 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 4. Обеспечение безопасности межсетевых соединений с применением шлюзов безопасности. Угрозы, методы проектирования и вопросы, касающиеся мер и средств контроля и управления
66. ГОСТ Р ИСО/МЭК 27033-5-2014 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 5. Обеспечение безопасности виртуальных частных сетей. Угрозы, методы проектирования и вопросы, касающиеся мер и средств контроля и управления.
67. ГОСТ Р ИСО/МЭК 27037-2014 Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме.
68. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.
69. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.
70. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.

71. РД 50-34.698-90 Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов.
72. ГОСТ Р ИСО/МЭК 18045-2008 Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий.
73. ГОСТ Р ИСО/МЭК 21827-2010 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Проектирование систем безопасности. Модель зрелости процесса.
74. ГОСТ Р ИСО/МЭК ТО 19791-2008 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем.
75. ГОСТ Р ИСО/МЭК ТО 15446-2008 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности.
76. ГОСТ Р ИСО/МЭК 21827-2010 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Проектирование систем безопасности. Модель зрелости процесса.
77. ГОСТ Р 54581-2011 Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности ит. Часть 1. Обзор и основы.
78. ГОСТ Р 53113.2-2009 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов.
79. ГОСТ Р 53115-2008 Защита информации. Испытание технических средств обработки информации на соответствие требованиям защищенности от несанкционированного доступа. Методы и средства.
80. ГОСТ Р 53112-2008 Защита информации. Комплексы для измерений параметров побочных электромагнитных излучений и наводок. Технические требования и методы испытаний.
81. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.
82. ГОСТ Р 53109-2008 Система обеспечения информационной безопасности сети связи общего пользования. Паспорт организации связи по информационной безопасности.
83. ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения.

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

1. Российская государственная библиотека. http://www.rsl.ru.
2. Государственная публичная научно-техническая библиотека России. http://www.gpntb.ru.
3. Библиотека МГТУ им. Н.Э. Баумана. http://library.bmstu.ru.
4. Научно-техническая библиотека КФ МГТУ им. Н.Э. Баумана. http://library.bmstu-kaluga.ru.
5. Научная электронная библиотека http://eLIBRARY.RU.
6. Электронно-библиотечная система издательства «Лань» http://e.lanbook.com.
7. Электронно-библиотечная система «Университетская библиотека онлайн» http://biblioclub.ru.
8. Электронно-библиотечная система «IPRbooks» http://www.iprbookshop.ru.

9. Образовательная платформа «Юрайт» https://urait.ru.

10. Электронно-библиотечная система «ibooks.ru» https://ibooks.ru.

11. Электронно-библиотечная система «Консультант студента» https://www.studentlibrary.ru.

12. Электронная библиотека «Grebennikon» https://grebennikon.ru.

13. Центральная библиотека образовательных ресурсов Минобрнауки РФ. www.edulib.ru.

14. Единая коллекция цифровых образовательных ресурсов http://school-collection.edu.ru.

15. Федеральный центр информационно-образовательных ресурсов. http://fcior.edu.ru.

16. Единая коллекция цифровых образовательных ресурсов http://school-collection.edu.ru.

17. Единое окно доступа к образовательным ресурсам. Раздел «Машиностроение» http://window.edu.ru/catalog/?p_rubr=2.2.75.11

18. Информационно-поисковая система «Первый машиностроительный портал» http://www.1bm.ru.

19. Портал машиностроения http://www.mashportal.ru.

11. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ СТУДЕНТОВ ПО ПРАКТИКЕ

Приступая к освоению дисциплины обучающийся должен принимать во внимание следующие положения.

Перед началом практики студент получает доступ к учебно-методическим материалам по дисциплине в электронной информационно-образовательной среде КФ МГТУ им. Н.Э. Баумана.

Практика – форма организации образовательной деятельности при освоении образовательной программы в условиях непосредственного выполнения обучающимися определенных видов работ, связанных с будущей профессиональной деятельностью и направленных на формирование, закрепление, развитие практических навыков и компетенций по профилю соответствующей образовательной программы.

Практика может быть организована:

- в организации, осуществляющей деятельность по профилю соответствующей образовательной программы, в том числе в структурном подразделении профильной организации;
- непосредственно в КФ МГТУ им. Н.Э. Баумана.

Обучающиеся, совмещающие обучение с трудовой деятельностью, вправе проходить практику по месту трудовой деятельности в случаях, если профессиональная деятельность, осуществляемая ими, соответствует требованиям образовательной программы к проведению практики.

Практика обучающихся с ограниченными возможностями здоровья и инвалидов организуется с учетом особенностей их психофизического развития, индивидуальных возможностей и состояния здоровья.

Оценивание результатов практики ведется в соответствии с Положением о текущем контроле успеваемости и промежуточной аттестации студентов КФ МГТУ им. Н.Э. Баумана на основе Фонда оценочных средств.

12. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ПРОВЕДЕНИИ ПРАКТИКИ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ И ПРОФЕССИОНАЛЬНЫХ БАЗ ДАННЫХ

Информационные технологии:

Электронная информационно-образовательная среда КФ 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.

Программное обеспечение:

1. LibreOffice.
2. КОМПАС (САПР)
3. AstraLinux

Информационные справочные системы:

1. Федеральное агентство по техническому регулированию и метрологии. Информационный портал https://www.rst.gov.ru/portal/gost.
2. Федеральный информационный фонд стандартов https://www.gostinfo.ru/pages/Maintask/fund.
3. Федеральный информационный фонд технических регламентов и стандартов https://www.gostinfo.ru/pages/Maintask/infsys.
4. Каталог государственных стандартов: Станки металлообрабатывающие https://internet-law.ru/gosts/1709/.
5. Каталог государственных стандартов. Инструмент промышленный и приспособления https://internet-law.ru/gosts/1647/.
6. Каталог национальных стандартов https://www.rst.gov.ru/portal/gost//home/standarts/catalognational.
7. Каталог межгосударственных стандартов https://www.rst.gov.ru/portal/gost//home/standarts/cataloginter.
8. Действующие технические регламенты https://www.rst.gov.ru/portal/gost//home/standarts/technicalregulationses.

Профессиональные базы данных:

9. Банк данных угроз безопасности информации. https://bdu.fstec.ru/
10. Государственный реестр сертифицированных средств защиты информации. https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00

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

1. Библиотеки и помещения для самостоятельной работы обучающихся, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде КФ МГТУ им. Н.Э. Баумана.

2. Для успешного прохождения практики на предприятии – базе практики должно быть организовано рабочее место обучающемуся (стол, стул, ПК), открыт доступ к документации (за исключением документации, содержащей государственную или коммерческую тайну), предоставлена возможность посещения производственных подразделений предприятия, отвечающих за реализацию результатов технологической подготовки производства (за исключением подразделений, выпускающих продукцию специального назначения).

Утверждена на заседании кафедры ИУК6

«Защита информации»

Протокол № 32.00-80-05/4 от 06.04.2023 г.

ЛИСТ ВНЕСЕНИЯ ИЗМЕНЕНИЙ

1). П.7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ, ЧИТАТЬ В СЛЕДУЮЩЕЙ РЕДАКЦИИ:

7. Перечень учебной литературы и дополнительных материалов, необходимых для освоения дисциплины

Литература по дисциплине:

1. Тумбинская, М. В. Защита информации на предприятии : учебное пособие / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2020. — 184 с. — ISBN 978-5-8114-4291-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/130184
2. Основы научного творчества Учебное пособие / Аверченков В.И., Малахов Ю.А. - 2012. - URL: http://www.iprbookshop.ru/7004.html.
3. Имитационное моделирование Учебное пособие. - 2019. - URL: http://www.iprbookshop.ru/101442.html.

2). П.10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ИЗУЧЕНИИ ДИСЦИПЛИНЫ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ЧИТАТЬ В СЛЕДУЮЩЕЙ РЕДАКЦИИ:

10. Перечень информационных технологий, используемых при изучении дисциплины, включая перечень программного обеспечения, информационных справочных систем и профессиональных баз данных

Программное обеспечение:

- LibreOffice

Преподаватель кафедры:

Твердова С.М., доцент (к.н.), кандидат технических наук, доцент, tverdovasm@bmstu.ru

Утверждена на заседании кафедры ИУК6

«Защита информации»

Протокол № 07.04.06-04.08/4 от 04.04.2024 г.

ЛИСТ ВНЕСЕНИЯ ИЗМЕНЕНИЙ

1). П.7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ, ЧИТАТЬ В СЛЕДУЮЩЕЙ РЕДАКЦИИ:

7. Перечень учебной литературы и дополнительных материалов, необходимых для освоения дисциплины

Литература по дисциплине:

1. Чернышов А. В. Организация и проведение преддипломной практики : учебно-методическое пособие / Чернышов А. В. ; МГТУ им. Н. Э. Баумана. (Нац. исслед. ун-т). - М. : Изд-во МГТУ им. Н. Э. Баумана, 2018. - 24 с. - ISBN 978-5-7038-4974-3.
2. Арсенькина Л. С., Манучарян А. К. Преддипломная практика : учебно-методическое пособие / Арсенькина Л. С., Манучарян А. К. ; МГТУ им. Н. Э. Баумана (национальный исследовательский ун-т). - М. : Изд-во МГТУ им. Н. Э. Баумана, 2020. - 20 с. : ил. - ISBN 978-5-7038-5442-6.
3. Организация и проведение преддипломной практики : учебно-методическое пособие / Шахнов В. А., Адамова А. А., Гриднев В. Н. [и др.] ; ред. Шахнов В. А. ; МГТУ им. Н. Э. Баумана. - М. : Изд-во МГТУ им. Н. Э. Баумана, 2018. - 21 с. - Библиогр. в конце брош. - ISBN 978-5-7038-4988-0.
4. Тумбинская, М. В. Защита информации на предприятии : учебное пособие / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2020. — 184 с. — ISBN 978-5-8114-4291-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/130184
5. Основы научного творчества Учебное пособие / Аверченков В.И., Малахов Ю.А. - 2012. - URL: http://www.iprbookshop.ru/7004.html.
6. Имитационное моделирование Учебное пособие. - 2019. - URL: http://www.iprbookshop.ru/101442.html.

2). П.10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ИЗУЧЕНИИ ДИСЦИПЛИНЫ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ЧИТАТЬ В СЛЕДУЮЩЕЙ РЕДАКЦИИ:

10. Перечень информационных технологий, используемых при изучении дисциплины, включая перечень программного обеспечения, информационных справочных систем и профессиональных баз данных

Программное обеспечение:
- LibreOffice
- Альт Образование

Преподаватель кафедры:

Твердова С.М., доцент (к.н.), кандидат технических наук, доцент, tverdovasm@bmstu.ru