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 ДИСЦИПЛИНЫ

Управление информационной безопасностью

Автор программы:
Гончаренко С.Н., профессор (д.н.), доктор технических наук, профессор, g_sn@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. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Настоящая рабочая программа дисциплины устанавливает планируемые результаты обучения по дисциплине, а также определяет содержание и виды учебных занятий 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 специальностей (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**
	Общепрофессиональные компетенции собственные
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-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-21 (10.05.03)	Способен управлять инцидентами информационной безопасности и реагировать на них, осуществлять контроль обеспечения информационной безопасности в организациях кредитно-финансовой сферы
ОПКС-22 (10.05.03)	Способен организовать защиту информации в автоматизированных системах и обеспечивать ее в ходе эксплуатации автоматизированных систем, задействованных в реализации технологических и бизнес-процессов организаций кредитно-финансовой сферы, в

	соответствии с нормативными правовыми актами и нормативными методическими документами Банка России в области защиты информации
ОПКС-28 (10.05.03)	Способен участвовать в создании системы обеспечения информационной безопасности автоматизированной системы в защищенном исполнении
	Профессиональные компетенции собственные (обязательные)
ПКСо-1 (10.05.03)	Способен разрабатывать проектные решения по защите информации в автоматизированных системах
	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 категорий «знать, уметь, владеть» планируется достижение результатов обучения по дисциплине (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**
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 су-	ЗНАТЬ - эксплуатацию автоматизированных систем в защищенном исполнении - типовые модели угроз и модели нарушителей информационной безопасности - особенности применения математических моделей, используемых в автоматизации проектирования автоматизированной системы с учетом требований по защите информации - требования к оформлению научно-технической документации - принципы и средства описания бизнес-процессов для разработки системы 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**

1	2	3
ществующих автоматизированных систем в соответствии с требованиями по защите информации	УМЕТЬ - проводить оценку эффективности применения средств защиты информации для заданных условий эксплуатации - выполнять анализ объекта проектирования и условий его применения - документировать структуру и принципы функционирования автоматизированной системы защиты информации ВЛАДЕТЬ - современными методами и средствами анализа и проектирования автоматизированной системы защиты информации - навыками комплексного рассмотрения вопросов конструкторского и технологического проектирования - методикой составления технико-экономического обоснования и технического задания на разработку системы защиты информации	
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	УМЕТЬ - разрабатывать проекты нормативных и организационно-распорядительных документов по защите информации ВЛАДЕТЬ - навыками создания и применения системы менеджмента информационной безопасности в организациях кредитно-финансовой сферы - навыками определения состава и содержания мер, направленных на обеспечение защиты информации для непрерывности выполнения бизнес- и технологических процессов организации кредитно-финансовой сферы и разработки планов по их реализации	**Формы обучения:** Фронтальная и групповая формы. **Методы обучения:** Методы практической работы (Практические занятия) Наблюдение и Исследовательский метод (Лабораторные работы) Метод проблемного обучения (Самостоятельная работа) **Активные и интерактивные методы обучения**

1	2	3
ОПКС-21 (10.05.03) Способен управлять инцидентами информационной безопасности и реагировать на них, осуществлять контроль обеспечения информационной безопасности в организациях кредитно-финансовой сферы	ЗНАТЬ - этапы менеджмента инцидентов информационной безопасности УМЕТЬ - организовывать работу по управлению инцидентами информационной безопасности и обеспечения ситуационной осведомленности организации кредитно-финансовой сферы	**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**
ОПКС-22 (10.05.03) Способен организовать защиту информации в автоматизированных системах и обеспечивать ее в ходе эксплуатации автоматизированных систем, задействованных в реализации технологических и бизнес-процессов организаций кредитно-финансовой сферы, в соответствии с нормативными правовыми актами и нормативными методическими документами Банка России в области защиты информации	УМЕТЬ - разрабатывать проекты нормативных и организационно-распорядительных документов по защите информации ВЛАДЕТЬ - навыками определения состава и содержания мер, направленных на обеспечение защиты информации в автоматизированных системах для непрерывности выполнения бизнес- и технологических процессов организации кредитно-финансовой сферы	**Формы обучения:** Фронтальная и групповая формы. **Методы обучения:** Наблюдение и Исследовательский метод (Лабораторные работы) Метод проблемного обучения (Самостоятельная работа) **Активные и интерактивные методы обучения**
ОПКС-28 (10.05.03) Способен участвовать в создании системы обеспечения информационной безопасности автоматизированной системы в защищенном исполнении	ВЛАДЕТЬ - навыками работы с современными системами автоматизированного проектирования	**Формы обучения:** Фронтальная и групповая формы. **Методы обучения:** Наблюдение и Исследовательский метод (Лабораторные работы) Метод проблемного обучения (Самостоятельная работа) **Активные и интерактивные методы обучения**

1	2	3
ПКСо-1 (10.05.03) Способен разрабатывать проектные решения по защите информации в автоматизированных системах	ЗНАТЬ - 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 УМЕТЬ - 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	**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**
ПКС-6 (10.05.03/41 Анализ безопасности информационных систем) Способен участвовать в разработке требований по защите, формировании политик безопасности компьютерных систем и сетей	ВЛАДЕТЬ - навыками формирования политик безопасности компьютерных систем и сетей	**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**

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина входит в Блок 1. «Дисциплины (модули)» образовательной программы и относится к обязательной части.

3. ОБЪЕМ ДИСЦИПЛИНЫ

Количество семестров освоения дисциплины: 1.

Общий объем дисциплины составляет 3 зачетных единиц (з.е.). В том числе: в 1-ом семестре – 3 з.е.

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

Виды учебной работы	**Всего**	**Объем по семестрам**
		1
Объем дисциплины	108	108
Аудиторная работа[1]	**68**	**68**
Лекции (Л)	34	34
Семинары (С)	-	-
Практические занятия (ПЗ)	-	-
Лабораторные работы (ЛР)	34	34
Самостоятельная работа (СР)	**40**	**40**
Проработка учебного материала лекций	4.25	4.25
Подготовка к выполнению и защите лабораторных работ	8	8
Подготовка к сдаче и сдача экзамена	-	-
Выполнение домашних работ	24	24
Подготовка к выполнению и выполнение контрольных работ	-	-
Другие виды самостоятельной работы, в том числе: - Самостоятельное дополнение конспекта	3,75 3,75	3,75 3,75

[1] Для дисциплин, участвующих в формировании профессиональных компетенций, аудиторная работа проводится в форме практической подготовки, организуемой путем проведения практических занятий, практикумов, лабораторных работ, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью, а также путем проведения занятий лекционного типа, предусматривающих передачу учебной информации обучающимся, необходимой для последующего выполнения работ, связанных с будущей профессиональной деятельностью

лекций		
Вид промежуточной аттестации		**Зачет**

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

Модули и проекты	**Неделя завершения модуля**	Виды учебных занятий				**Итого, ак.час**
		Лекции, ак.час.	Практические занятия (семинары), ак.час.	Лабораторные работы, ак.час.	Самостоятельная работа, ак.час.	
1 семестр		**34**	**-**	**34**	**40**	**108**
Модуль 1 «Основные понятия управления информационной безопасностью»	**8**	16	-	16	20	**52**
Модуль 2 «Разработка и реализация систем управления информационной безопасностью»	**17**	18	-	18	20	**56**

Содержание дисциплины, структурированное по видам занятий (темам)

Модуль 1 «Основные понятия управления информационной безопасностью»

№, п/п	**Лекции – 16 час.**
Л 1.1	**Понятие управления – 2 час.** Основные определения. Необходимость управления информационной безопасностью. Место управления информационной безопасностью в системе управления предприятием.
Л 1.2	**Подходы к управлению – 2 час.** Системный подход. Процессный подход. Системный подход к управлению организацией. Процессный подход к управлению организацией.
Л 1.3	**Стандартизация систем и процессов управления ИБ – 2 час.** Серия стандартов ISO/IEC 27000 «Информационные технологии. Методы обеспечения безопасности». Стандарты на отдельные процессы управления ИБ и оценку безопасности. Отраслевые стандарты в области управления ИБ.
Л 1.4	**Понятие системы управления информационной безопасностью – 2 час.**

Л 1.5	**Практические правила управления ИБ – 2 час.**
Л 1.6	**Внедрение системы управления ИБ – 2 час.** Руководство по внедрению системы управления ИБ
Л 1.7	**Аудит системы управления ИБ – 2 час.** Руководство по аудиту системы управления ИБ
Л 1.8	**Управление ИБ как инструмент управления непрерывностью бизнеса – 2 час.** Общие критерии и методология оценки безопасности информационных технологий. Управление непрерывностью бизнеса.
	Лабораторные работы – 16 час.
ЛР 1.1	**Исследование российских и международных стандартов управления ИБ – 6 час**.
ЛР 1.2	**Изучение приемов работы с пакетом компьютерного моделирования – 10 час.**
	Самостоятельная работа – 20 час.
СР 1.1	**Проработка учебного материала лекций – 2 час.** Аналитическая работа с конспектом лекций, доработка конспекта
СР 1.2	**Подготовка к выполнению/защите лабораторных работ – 4 час.** Изучение методических указаний, составление отчета по лабораторным работам, проработка контрольных вопросов.
СР 1.3	**Выполнение домашней работы по модулю «***Разработка системы управления информационной безопасностью предприятия***» – 12 час.**
СР 1.4	**Самостоятельное дополнение конспекта лекций – 2 час.** Дополнение конспекта лекций из рекомендованных источников

Модуль 2 «Разработка и реализация систем управления информационной безопасностью»

	Лекции – 18 час.
Л 2.1	**Представление информации в ЭВМ - 2 час.** Общие вопросы представления информации в ЭВМ. Представление числовой информации в ЭВМ. Представление целых чисел. Прямой код. Дополнительный код. Представление чисел с плавающей запятой. Представление символьной информации в ЭВМ. Кодировка ASCII. Кодировка Unicode. Представление графической информации в ЭВМ
Л 2.2	**Логические основы ЭВМ - 2 час.**

	Логические функции одной переменной. Логические функции двух переменных. Системы логических элементов
Л 2.3	**Архитектура персонального компьютера - 2 час.** Принстонская (неймановская) и гарвардская архитектуры. Основные компоненты. Основные функции и характеристики.
Л 2.4	**Представление информации в ЭВМ - 2 час.** Общие вопросы представления информации в ЭВМ. Представление числовой информации в ЭВМ. Представление целых чисел. Прямой код. Дополнительный код. Представление чисел с плавающей запятой. Представление символьной информации в ЭВМ. Кодировка ASCII. Кодировка Unicode. Представление графической информации в ЭВМ
Л 2.5	**Логические основы ЭВМ - 2 час.** Логические функции одной переменной. Логические функции двух переменных. Системы логических элементов
Л 2.6	**Архитектура персонального компьютера - 2 час.** Принстонская (неймановская) и гарвардская архитектуры. Основные компоненты. Основные функции и характеристики.
Л 2.7	**Представление информации в ЭВМ - 2 час.** Общие вопросы представления информации в ЭВМ. Представление числовой информации в ЭВМ. Представление целых чисел. Прямой код. Дополнительный код. Представление чисел с плавающей запятой. Представление символьной информации в ЭВМ. Кодировка ASCII. Кодировка Unicode. Представление графической информации в ЭВМ
Л 2.8	**Логические основы ЭВМ - 2 час.** Логические функции одной переменной. Логические функции двух переменных. Системы логических элементов
Л 2.9	**Архитектура персонального компьютера - 2 час.** Принстонская (неймановская) и гарвардская архитектуры. Основные компоненты. Основные функции и характеристики.
	Лабораторные работы – 18 час.
ЛР 2.1	**Разработка частной политики безопасности – 8 час.**
ЛР 2.2	**Построение системы управления ИБ – 10 час.**
	Самостоятельная работа – 20 час.
СР 2.1	**Проработка учебного материала лекций – 2,25 час.** Аналитическая работа с конспектом лекций, доработка конспекта
СР 2.2	**Подготовка к выполнению/защите лабораторных работ – 4 час.** Изучение методических указаний, составление отчета по лабораторным работам, проработка контрольных вопросов.

СР 2.3	**Выполнение домашней работы по модулю «Оформление пакета документов по организации управления информационной безопасностью» – 12 час.**
СР 2.4	**Самостоятельное дополнение конспекта лекций – 1,75 час.** Дополнение конспекта лекций из рекомендованных источников

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

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

1. Рабочая программа дисциплины.
2. Учебная литература и дополнительные материалы [Раздел 7 Рабочей программы дисциплины].
3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» [Раздел 8 Рабочей программы дисциплины].
4. Методические указания для обучающихся по освоению дисциплины [Раздел 9 Рабочей программы дисциплины], обеспечивающие самостоятельную работу студента при:
   - подготовке к аттестациям,
   - выполнении домашних работ,
   - подготовке к лабораторным работам.
5. Комплект индивидуальных заданий.

Студенты начинают получать доступ к указанным материалам начиная с первого занятия по дисциплине.

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 (раздел 1). 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, 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 дисциплины.

В основу системы оценок положен принцип декомпозиции дисциплины на модули и формирование итоговой оценки в течение семестра путем накопления студентом баллов за различные виды учебных работ и контрольных мероприятий.

Оценка результатов обучения

Модули, виды учебных работ и контрольных мероприятий	Баллов	
	минимум	максимум
Модуль 1 «Основные понятия управления информационной безопасностью»	**29**	**49**
Посещение аудиторных занятий	6	8
Лабораторный практикум	16	28
Домашняя работа	7	13
Модуль 2 «Разработка и реализация систем управления информационной безопасностью»	**31**	**51**
Посещение аудиторных занятий	7	9
Лабораторный практикум	16	28
Домашняя работа	8	14
Итого	**60**	**100**

Промежуточная аттестация

Формой промежуточной аттестации по дисциплине является **зачёт**.

Суммарное количество баллов, начисленных студенту по итогам выполнения им всех видов учебной работы и контрольных мероприятий, предусмотренных программой дисциплины, представляет собой балльную оценку по дисциплине. Перевод балльной оценки в недифференцированную оценку осуществляется в соответствии с таблицей.

Балльная оценка по дисциплине	Недифференцированная оценка результатов промежуточной аттестации
90 – 100	Зачтено
75 – 89	
60 – 74	
0-59	Не зачтено

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

Литература по дисциплине

1. Управление информационной безопасностью Учебное пособие / Шилов А.К. - 2018. - URL: http://www.iprbookshop.ru/87643.html.
2. Информационная безопасность. Национальные стандарты Российской Федерации. 2-е изд. Учебное пособие Ю. А. Родичев / Родичев Ю. А. - URL: https://ibooks.ru/reading.php?short=1&productid=359451.
3.Искусство защиты и взлома информации Д. Скляров / Скляров Д. - URL: https://ibooks.ru/reading.php?short=1&productid=335110.
4. Ерохин, В. В. Безопасность информационных систем : учебное пособие / В. В. Ерохин, Д. А. Погонышева, И. Г. Степченко. — 4-е изд., стер. — Москва : ФЛИНТА, 2022. — 184 с. — ISBN 978-5-9765-1904-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/232457

Дополнительные материалы

5. Стратегия национальной безопасности РФ.
6. Доктрина информационной безопасности РФ.
7. Серия стандартов ISO/IEC 27000 «Информационные технологии. Методы обеспечения безопасности».

8. 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.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ СТУДЕНТОВ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

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

Дисциплина построена по модульному принципу, каждый модуль представляет собой логически завершенный раздел курса.

На первом занятии студент получает доступ к учебно-методическим материалам по дисциплине в электронной информационно-образовательной среде КФ МГТУ им. Н.Э. Баумана.

Лекционные занятия посвящены рассмотрению ключевых, базовых положений курса и разъяснению учебный заданий, выносимых на самостоятельную проработку.

Лабораторные работы предназначены для приобретения умений и навыков для решения практических задач в предметной области дисциплины.

Самостоятельная работа студентов включает усвоение и расширение материалов лекционного курса на основе поиска, анализа, структурирования и представления в компактном виде современной информации их всех возможных источников; выполнение домашних работ по модулям; подготовку к аттестации; подготовку к лабораторным работам.

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

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 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:

- LibreOffice.
- AstraLinux

Информационные справочные системы:

1. Информационно-правовая система «Гарант» http://www.garant.ru;
2. Информационно-правовая система «Консультант Плюс» http://www.consultant.ru.

Профессиональные базы данных:

1. Каталог национальных стандартов https://www.rst.gov.ru/portal/gost//home/standarts/catalognational.
2. Каталог межгосударственных стандартов https://www.rst.gov.ru/portal/gost//home/standarts/cataloginter.
3. Официальный сайт Федеральной службы по техническому и экспортному контролю. http://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	Учебные аудитории КФ МГТУ им. Н.Э. Баумана, укомплектованные специализированной мебелью и средствами обучения, служащими для представления учебной информации большой аудитории
2	Лабораторные работы	Лаборатории кафедры «Защита информации» КФ МГТУ им. Н.Э. Баумана, укомплектованные специализированной мебелью, оборудованием и техническими средствами для получения студентами необходимых умений и владений: - компьютеры с возможностью выход а в Интернет.
	Самостоятельная работа	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

12. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ, ИСПОЛЬЗУЕМЫЕ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Компетентностный подход при освоении дисциплины реализуется через использование в учебном процессе активных методов обучения – таких взаимных действий преподавателя и обучающихся, которые побуждают последних к активной мыслительной и практической деятельности в процессе овладения изучаемым материалом. При экстрактивном режиме обучения студент выступает только в роли обучаемого, при интерактивном режиме обучения – студент вовлекается во взаимонаправленные информационные потоки: студент – группа студентов – преподаватель.

В интерактивных режимах по дисциплине проводятся:

– Поисковые лабораторные работы по темам ЛР 1.1 – ЛР 2.2.

Формируются умения делать теоретические выводы на основе наблюдаемых явлений, навыки использования методов физического и математического моделирования и анализа при решении конкретных задач. Организуется беседа преподавателя и студентов для обсуждения результатов работы, формулирования обобщений и закономерностей.

– **Лекция проблемная** по темам Л 1.1; Л 1.8; Л 2.1-2.6.

Лектор совместно со студентами формулируют проблему и в ходе организуемого активного диалога ищут способы решения проблемы, формулируют новое знание (лекция-диалог).

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. Управление информационной безопасностью Учебное пособие / Шилов А.К. - 2018. - URL: http://www.iprbookshop.ru/87643.html.
2. Ерохин, В. В. Безопасность информационных систем : учебное пособие / В. В. Ерохин, Д. А. Погонышева, И. Г. Степченко. — 4-е изд., стер. — Москва : ФЛИНТА, 2022. — 184 с. — ISBN 978-5-9765-1904-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/232457

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:

Лачихина А.Б., доцент (к.н.), кандидат технических наук, доцент, lachikhinaab@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. Сабанов А. Г. Основы аутентификации субъектов доступа : учебное пособие / Сабанов А. Г. ; МГТУ им. Н. Э. Баумана (национальный исследовательский ун-т). - М. : Изд-во МГТУ им. Н. Э. Баумана, 2021. - 58 с. : рис., табл. - Библиогр.: с. 56-58. - ISBN 978-5-7038-5727-4.
2. Управление информационной безопасностью Учебное пособие / Шилов А.К. - 2018. - URL: http://www.iprbookshop.ru/87643.html.
3. Ерохин, В. В. Безопасность информационных систем : учебное пособие / В. В. Ерохин, Д. А. Погонышева, И. Г. Степченко. — 4-е изд., стер. — Москва : ФЛИНТА, 2022. — 184 с. — ISBN 978-5-9765-1904-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/232457

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

Преподаватели кафедры:

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

Петрищев Н.В., старший преподаватель, pnv@bmstu.ru