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

Методы антивирусной защиты

Авторы программы:
Жарова О.Ю., старший преподаватель, zharova@bmstu.ru
Лачихина А.Б., доцент (к.н.), кандидат технических наук, доцент, lachikhinaab@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.

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 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**
	Общепрофессиональные компетенции собственные
ОПКС-13 (10.05.03)	Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ действующих политик безопасности, выявлять и проводить анализ уязвимостей систем защиты информации, разрабатывать методы их устранения, в том числе за счет применения технических и организационных мер, проводить оценку достаточности реализованных мер 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
ОПКС-25 (10.05.03)	Способен планировать и проводить анализ защищенности и верификацию программного обеспечения информационных систем
	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-13 (10.05.03) Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ действующих политик безопасности, выявлять и проводить анализ уязвимостей систем защиты информации, разрабатывать методы их устранения, в том числе за счет применения технических и организационных мер, проводить оценку достаточности реализованных мер защиты информации	ЗНАТЬ - свойства защищаемой информации - типовые уязвимости средств защиты информации, методики и тесты для анализа степени защищенности средств защиты информации, соответствия нормативным требованиям по защите информации - типовые модели угроз и модели нарушителей информационной безопасности - методы и способы устранения уязвимостей УМЕТЬ - разрабатывать модели угроз и модели нарушителей информационной безопасности процессов создания и эксплуатации автоматизированных систем в защищенном исполнении - разрабатывать методики и тесты для анализа степени защищенности средств защиты информации в соответствии с нормативными требованиями по защите информации ВЛАДЕТЬ	**Формы обучения:** Фронтальная и групповая формы. **Методы обучения:** Словесный метод обучения (Лекции) Методы практической работы (Практические занятия) Наблюдение и Исследовательский метод (Лабораторные работы) Метод проблемного обучения (Самостоятельная работа) **Активные и интерактивные методы обучения**

1	2	3
	- навыками анализа наличия уязвимостей в системе защиты информации автоматизированных систем - навыками использования средств автоматизированного тестирования при разработке новых программных средств - навыками устранения выявленных уязвимостей	
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 - применять методы и средства обеспечения безопасности информации ВЛАДЕТЬ - 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**
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 - классификацию мероприятий по анализу защищенности программного обеспечения информационных систем - инструментарий анализа безопасности программного обеспечения УМЕТЬ - определять угрозы защищенности компьютерных систем	**Формы обучения:** Фронтальная и групповая формы. **Методы обучения:** Словесный метод обучения (Лекции) Методы практической работы (Практические занятия) Наблюдение и Исследовательский метод (Лабораторные работы)

1	2	3
	- выбирать необходимое инструментальное средство для выполнения анализа безопасности ПО ВЛАДЕТЬ - навыками организации защиты информации на объектах информатизации - навыками работы с инструментарием анализа безопасности программного обеспечения	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	ЗНАТЬ - методику формирования политики безопасности	**Формы обучения:** Фронтальная и групповая формы. **Методы обучения:** Словесный метод обучения (Лекции) 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 зачетные единицы (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]	**85**	**85**
Лекции (Л)	34	34
Семинары (С)	-	-
Практические занятия (ПЗ)	17	17
Лабораторные работы (ЛР)	34	34
Самостоятельная работа (СР)	**23**	**23**
Проработка учебного материала лекций	4,25	4,25
Подготовка к выполнению и защите лабораторных работ	8	8
Подготовка к практическим занятиям (семинарам)	2	2
Подготовка к сдаче и сдача экзамена	-	-
Выполнение домашних работ	-	-
Подготовка к выполнению и выполнение контрольных работ	6	6
Другие виды самостоятельной работы, в том числе: - Самостоятельное дополнение конспекта лекций	2,75 2,75	2,75 2,75
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] *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*

1 семестр		**34**	**17**	**34**	**23**	**108**
Модуль 1 «Антивирусное программное обеспечение»	**10**	20	10	20	13	**63**
Модуль 2 «Антивирусные песочницы и вирусные технологии»	**17**	14	7	14	10	**45**

Содержание дисциплины, структурированное по видам занятий (темам)

Модуль 1 «Антивирусное программное обеспечение»

№, п/п	**Лекции – 20 час.**
Л 1.1	**Средства антивирусной защиты – 2 час.** Риски при отсутствии эффективной антивирусной защиты
Л 1.2	**Организация антивирусной защиты. - 2 час.** Организация антивирусной защиты на предприятиях различного уровня защищенности и размера.
Л 1.3	**Классификация методов антивирусной защиты. - 2час.** Виды классификаций.
Л 1.4	**Методы обнаружения вирусов. - 2 час.** Методы обнаружения вирусов в ОС без использования антивирусных средств.
Л 1.5	**Классификация антивирусов. - 2 час.** Классификация антивирусов по типу.
Л 1.6	**Классификация антивирусов по изменяемости во времени. - 2 час.**
Л 1.7	**Антивирусные комплексы. - 2 час.** Состав антивирусных комплексов, различие и преимущества. Определение допустимой нагрузки на аппаратные средства вычислительных систем
Л 1.8	**Проблемы традиционного антивирусного ПО. - 2 час**. Архитектура толстого клиента.
Л 1.9	**Антивирусная защита из облака – 2 час.** Архитектура тонкого клиента.
Л 1.10	**Виды анализов. – 2 час.** Сигнатурный и поведенческий анализ. Виды сигнатурного анализа. Эвристика.
	Практические занятия – 10 час.
ПЗ 1.1	**Основные методы и механизмы защиты компьютерных систем. – 2 час.**
ПЗ 1.2	**Определение заражения вирусным ПО без использования антивирусов – 2 час.**
ПЗ 1.3	**Развертывание антивирусного комплекса. – 2 час.**
ПЗ 1.4	**Методы выбора оптимального антивирусного ПО для вычислительной системы с заданной мощностью. – 2 час.**
ПЗ 1.5	**Сравнение антивирусных технологий. – 2 час.**

	Лабораторные работы – 20 час.
ЛР 1.1	**Реализация политик антивирусной безопасности. - 16 час.**
ЛР 1.2	**Оценка экономической эффективности затрат на антивирусную защиту информации. 4 - час.**
	Самостоятельная работа – 13 час.
СР 1.1	**Проработка учебного материала лекций – 2,25 час.** Аналитическая работа с конспектом лекций, доработка конспекта
СР 1.2	**Подготовка к выполнению/защите лабораторных работ – 5 час.** Изучение методических указаний, составление отчета по лабораторным работам, проработка контрольных вопросов.
СР 1.3	**Подготовка к практическим занятиям – 1 час.** Изучение конспекта лекций, разделов учебников и учебных пособий, материалов предыдущих занятий.
СР 1.4	**Подготовка к выполнению контрольной работы – 3 час.** Повторение материала по пройденным разделам дисциплины. Контрольная работа проводится в форме письменного выполнения индивидуального задания.
СР 1.5	**Самостоятельное дополнение конспекта лекций – 1,75 час.** Дополнение конспекта лекций из рекомендованных источников

Модуль 2 «Антивирусные песочницы и вирусные технологии»

	Лекции – 14 час.
Л 2.1	**Антивирусные песочницы. – 2 час.** Определение. Виды изоляций. Режимы использования антивирусных песочниц.
Л 2.2	**Методы принятия решения о помещении под защиту – 2 час.**
Л 2.3	**Структура исполняемого файла.– 2 час.**
Л 2.4	**Вирусные технологии. Технологии заражения - 2 час.** Виды заражения исполняемых файлов. Дроппер. Инфектор. Инжектор. Лоадер.
Л 2.5	**Процесс заражения. – 2 час.** Инфицирование файловых объектов. Методы обеспечения автоматического запуска. Перехват вызовов функций.
Л 2.6	**Инжекты. – 2 час.** Виды инжектирования.
Л 2.7	**Наиболее опасные современные вирусы. – 2 час.**

	Подробное рассмотрение наиболее опасных вирусов.
	Практические занятия – 7 час.
ПЗ 2.1	**Изучение структуры заданного исполняемого файла – 2 час.**
ПЗ 2.2	**Анализ и излечение полиморфного вируса - 2 час.**
ПЗ 2.3	**Изучение технологии инжектирования – 3 час.**
	Лабораторные работы – 14 час.
ЛР 2.1	**Классификация мер обеспечения антивирусной защиты информации. АСОИ . – 4 час.**
ЛР 2.2	**Изучение работы вредоносного программного обеспечения. – 10 час.**
	Самостоятельная работа – 10 час.
СР 2.1	**Проработка учебного материала лекций – 2 час.** Аналитическая работа с конспектом лекций, доработка конспекта
СР 2.2	**Подготовка к выполнению/защите лабораторных работ – 3 час.** Изучение методических указаний, составление отчета по лабораторным работам, проработка контрольных вопросов.
СР 2.3	**Подготовка к практическим занятиям – 1 час.** Изучение конспекта лекций, разделов учебников и учебных пособий, материалов предыдущих занятий.
СР 2.4	**Подготовка к выполнению контрольной работы – 3 час.** Повторение материала по пройденным разделам дисциплины. Контрольная работа проводится в форме письменного выполнения индивидуального задания.
СР 2.5	**Самостоятельное дополнение конспекта лекций – 1 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 контрольным мероприятиям,
– подготовке к практическим и 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	Баллов	
	минимум	максимум
Модуль 1 «Антивирусное программное обеспечение»	**30**	**50**
Посещение аудиторных занятий	9	14
Лабораторный практикум	14	24
Контрольная работа	7	12

Модуль 2 «Антивирусные песочницы и вирусные технологии**»**	**30**	**50**
Посещение аудиторных занятий	9	14
Лабораторный практикум	14	24
Контрольная работа	7	12
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	Незачтено

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

Литература по дисциплине

1. Михайлов, А. В. Компьютерные вирусы и борьба с ними : практическое пособие / А. В. Михайлов. – 4-е изд., испр. и доп. – Москва : Диалог-МИФИ, 2012. – 148 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=136089 (дата обращения: 17.05.2021). – ISBN 978-5-86404-236-6. – Текст : электронный.
2. Алексеев, П. П. Антивирусы : настраиваем защиту компьютера от вирусов / П. П. Алексеев, Д. А Козлов, Р. Г. Прокди. — Санкт-Петербург : Наука и Техника, 2008. — 80 с. — ISBN 978-5-94387-604-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/35387.html (дата обращения: 17.05.2021). — Режим доступа: для авторизир. пользователей
3. Антивирусная защита компьютерных систем / Национальный Открытый Университет "ИНТУИТ". – Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2007. – 282 с. : ил. – Режим доступа: по подписке. –

URL: https://biblioclub.ru/index.php?page=book&id=233568 (дата обращения: 17.05.2021). – Текст : электронный.

4. Климентьев, К. Е. Компьютерные вирусы и антивирусы: взгляд программиста / К. Е. Климентьев. — Москва : ДМК Пресс, 2013. — 656 с. — ISBN 978-5-94074-885-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/63192
5. Компьютерные вирусы изнутри и снаружи К Касперски / Касперски К. - URL: https://ibooks.ru/reading.php?short=1&productid=21495.
6. Защита компьютерной информации. Эффективные методы и средства / Шаньгин В.Ф. - 2019. - URL: http://www.iprbookshop.ru/87992.html.

Дополнительные материалы

1. Стратегия национальной безопасности РФ.
2. Доктрина информационной безопасности РФ.

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.

Практические занятия проводятся для закрепления усвоенной информации, приобретения в основном умений, а в ряде случаев и навыков, решения практических задач в предметной области дисциплины.

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; подготовку к выполнению контрольных работ; подготовку к лабораторным работам и практическим занятиям.

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 ресур-

сам, 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,
– Code::Blocks.
– 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	Практические занятия	Учебные аудитории КФ МГТУ им. Н.Э. Баумана, укомплектованные специализированной мебелью и средствами обучения, необходимыми для получения студентами необходимых умений и владений
3	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.
4	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 1.2, 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 2.7.

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. Климентьев, К. Е. Компьютерные вирусы и антивирусы: взгляд программиста / К. Е. Климентьев. — Москва : ДМК Пресс, 2013. — 656 с. — ISBN 978-5-94074-885-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/63192
2. Защита компьютерной информации. Эффективные методы и средства / Шаньгин В.Ф. - 2019. - URL: http://www.iprbookshop.ru/87992.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

Преподаватели кафедры:

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

Жарова О.Ю., старший преподаватель, zharova@bmstu.ru