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

Безопасность операционных систем

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 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-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-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

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 - навыками анализа наличия уязвимостей в системе защиты информации автоматизированных систем - навыками использования средств автоматизированного тестирования при разработке новых программных средств - навыками устранения выявленных уязвимостей	**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-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:** Наблюдение и Исследовательский метод (Лабораторные работы) Метод проблемного обучения

1	2	3
		(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 - применять методы и средства обеспечения безопасности информации ВЛАДЕТЬ - навыками выбора и применения способов и средств защиты информации - 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 си-	ЗНАТЬ - основные угрозы и механизмы обеспечения информационной безопасности в современных технологиях	**Формы обучения:** Фронтальная и групповая формы. **Методы обучения:** Словесный метод обучения (Лекции) Метод проблемного обучения (Самостоятельная работа)

1	2	3
стемы в защищенном исполнении		**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 6 зачетных единиц (з.е.). В том числе:

в 1-ом семестре – 6 з.е.

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

Виды учебной работы	Всего	Объем по семестрам
		1
Объем дисциплины	216	216
Аудиторная работа[1]	**51**	**51**
Лекции (Л)	34	34
Семинары (С)	-	-
Практические занятия (ПЗ)	-	-
Лабораторные работы (ЛР)	17	17
Самостоятельная работа (СР)	**165**	**165**
Проработка учебного материала лекций	4.25	4.25
Подготовка к выполнению и защите лабораторных работ	10	10
Подготовка к сдаче и сдача экзамена	36	36
Выполнение домашних работ	3	3
Подготовка к выполнению и выполнение контрольных работ	3	3
Выполнение курсового проекта/работы (КП/КР)	108	108
Другие виды самостоятельной работы, в том числе: - Самостоятельное дополнение конспекта лекций	0.75 0.75	0.75 0.75

[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

Вид промежуточной аттестации		**Экзамен** **ДЗчт**

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**	**-**	**17**	**165**	**216**
Модуль 1 «Угрозы и вредоносное ПО»	**10**	20	-	10	11	**41**
Модуль 2 «Средства защиты»	**17**	14	-	7	10	**31**
Курсовой проект «Обеспечения безопасности в операционных системах»					108	**108**
Подготовка/сдача экзамена					36	**36**

Содержание дисциплины, структурированное по видам занятий (темам)

Модуль 1 «Угрозы и вредоносное ПО»

№, п/п	**Лекции – 20 час.**
Л 1.1	**Введение. Угрозы. – 2 час.** Рассматриваются такие понятия, как угроза, защищенная система. Приводится классификация существующих угроз в ОС различного характера.
Л 1.2	**Вредоносное ПО. Троянские программы. – 2 час.** Классификация вредоносного ПО. Понятие, принцип функционирования троянской программы, способы устранения. Понятие, принцип функционирования шпионской программы, способы устранения.
Л 1.3	**Вредоносное ПО. Руткит. Backdoor. – 2 час.** Понятие, принцип функционирования руткита, способы устранения. Понятие, принцип функционирования вредоносного ПО типа Backdoor, способы устранения.
Л 1.4	**Вредоносное ПО. Вирусы. - 2 час.** Понятие, принцип функционирования программного вируса, способы устранения. Понятие, принцип функционирования вредоносного ПО типа Червь, способы устранения.
Л 1.5	**Использование дефектов программного кода. Переполнение буфера и целочисленных значений. – 2 час.** Принципы использования дефектов программного пода, эксплуатация уязвимостей типа: внедрение программного кода.
Л 1.6	**Использование дефектов программного кода. Внедрение программного кода. Эскалация привилегий. – 2 час.** Принципы использования дефектов программного пода, эксплуатация уязвимостей типа: эскалация привилегий.

Л 1.7	**Инсайдерские атаки. Логические бомбы. Лазейки. Фальсификация входа в систему. – 2 час.** Виды атак: логические бомбы, лазейки, фальсификация входа в систему.
Л 1.8	**Инсайдерские атаки. Общий подход к решению проблемы инсайдерских атак. - 2 час.** Подход к решению проблемы инсайдерских атак в целом, основные механизмы за-щиты.
Л 1.9	**Инсайдерские атаки. Требования к локализации компьютерных ресурсов. – 2 час.** Подход к решению проблемы инсайдерских атак. Требования к локализации компьютерных ресурсов.
Л 1.10	**Инсайдерские атаки. Общие требования к организации ограничительной политики доступа к ресурсам. – 2 час.** Подход к решению проблемы инсайдерских атак на основе общих требований к организации ограничительной политики доступа к ресурсам.
	Лабораторные работы – 10 час.
ЛР 1.1	**Изучение методики полного перебора (брутфорс). - 4 час.**
ЛР 1.2	**Изучение методов использования программных ловушек (хуков). - 4 час.**
ЛР 1.3	**Изучение методов хранения локальных данных браузерами. - 2 час.**
	Самостоятельная работа – 11 час.
СР 1.1	**Проработка учебного материала лекций – 2 час.** Аналитическая работа с конспектом лекций, доработка конспекта
СР 1.3	**Подготовка к выполнению/защите лабораторных работ – 6 час.** Изучение методических указаний, составление отчета по лабораторным работам, проработка контрольных вопросов.
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.

Модуль 2 «Средства защиты»

	Лекции – 14 час.
Л 2.1	**Средства защиты. - 2 часа.** Классификация средств защиты, их применение. Возможности и уровень защиты ОС при использовании различных программных продуктов.
Л 2.2	**Внутренние механизмы защиты ОС. Общие понятия. – 2 часа.** Рассматривается такие понятия, как аутентификация и авторизация. Назначение, использование, практическое применение механизмов аутентификации и авторизации.
Л 2.3	**Критерии оценки заслуживающих доверия компьютерных систем - 2 час.** Оценка безопасности как стандартизированный процесс. Критерии оценки. Общие критерии.
Л 2.4	**Системные компоненты безопасности – 2 час.** Рассмотрение существующих в ОС компонентов безопасности.

Л 2.5	**Взаимодействие компонентов безопасности ОС. - 2 час.**
Л 2.6	**Защита объектов – 2 час.** Рассмотрение объектов ОС и способов защиты.
Л 2.7	**Уровни целостности. – 2 час.**
	Лабораторные работы – 7 час.
ЛР 2.1	**Изучение методов применения пакетных файлов для устранения последствий инфицирования носителей информации – 3 час.**
ЛР 2.2	**Изучение методов хранения паролей пользователей операционной системы Windows. – 4 час.**
	Самостоятельная работа – 10 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	**Самостоятельное дополнение конспекта лекций – 0,75 час.** Дополнение конспекта лекций из рекомендованных источников
СР 2.4	**Выполнение домашней работы «Изучение уязвимостей pdf-файлов» – 3 час.**

Курсовой проект «Обеспечения безопасности в операционных системах»

КП 1	**Курсовой проект «Обеспечения безопасности в операционных системах» – 108 час.**

СРЭ 1	**Подготовка и сдача экзамена – 36 час.** Повторение освоенного материала по разделам дисциплины, обобщение и систематизация полученных знаний, самостоятельная проработка практических умений и навыков – 36 час.

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 и аттестациям,
- выполнении домашних работ,
- подготовке к лабораторным работам;

– выполнении курсового проекта.

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 «Угрозы и вредоносное ПО**»**	**23**	**40**
Посещение аудиторных занятий	12	20
Лабораторный практикум	9	15
Контрольная работа	2	5
Модуль 2 «Средства защиты**»**	**19**	**30**
Посещение аудиторных занятий	8	13
Лабораторный практикум	6	10
Домашняя работа	5	7
Подготовка/сдача экзамена	**18**	**30**
Итого	**60**	**100**

Промежуточная аттестация

Формой промежуточной аттестации по дисциплине является **экзамен**. На экзаменационную составляющую балльной оценки по дисциплине выделяется 30 баллов из 100. Экзамен, как процедура оценивания способности студента обобщать и систематизировать

учебный материал, считается сданным, если студент получил за выполнение экзаменационных заданий не менее 18 баллов.

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

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

Формой промежуточной аттестации за курсовой проект по дисциплине является **дифференцированный зачёт**.

Перевод балльной оценки в дифференцированную оценку осуществляется в соответствии с таблицей.

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

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

Литература по дисциплине

1. Жидков, О. М. Сетевые операционные системы / О. М. Жидков. – Москва : Лаборатория книги, 2011. – 114 с. : табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=142238
2. Средства безопасности операционной системы ROSA Linux Учебное пособие / Ложников П.С., Провоторский А.О. - 2017. - URL: http://www.iprbookshop.ru/78474.html .
3. Средства безопасности операционной системы Windows Server 2008 Учебно-методическое пособие / Глотина И.М. - 2018. - URL: http://www.iprbookshop.ru/72538.html .

Дополнительные материалы

8. Стратегия национальной безопасности РФ.

9. Доктрина информационной безопасности РФ.
10. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.

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 выполнению контрольных мероприятий и аттестации; подготовку к практическим занятиям и 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
- 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
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 1.1; 2.1; 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;1.2.

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. Средства безопасности операционной системы ROSA Linux Учебное пособие / Ложников П.С., Провоторский А.О. - 2017. - URL: http://www.iprbookshop.ru/78474.html.
2. Средства безопасности операционной системы Windows Server 2008 Учебно-методическое пособие / Глотина И.М. - 2018. - URL: http://www.iprbookshop.ru/72538.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:

- Debian Linux
- LibreOffice

Преподаватели кафедры:

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

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