ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ИНКЛЮЗИВНОГО ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет Прикладной математики и информатики
Кафедра Цифровых технологий

УТВЕРЖДАЮ
Проректор по учебно-методической работе
_____ Сахарчук Е.С.
«27» 09 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
ЗАЩИТА В ОПЕРАЦИОННЫХ СИСТЕМАХ

образовательная программа направления подготовки
09.04.03 "Прикладная информатика"
Б1.В.03 «Дисциплины (модули)», Часть, формируемая участниками образовательных отношений, Дисциплины (модули) по выбору

Профиль подготовки
Прикладная информатика в информационной сфере

Квалификация (степень) выпускника:

Магистр

Форма обучения: очная

Курс 2 семестр 3, 4

Москва 2022

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования направления 09.04.03 "Прикладная информатика", утвержденного приказом Министерства науки и высшего образования Российской Федерации № 916 от «19» сентября 2017 г.

Разработчик рабочей программы:
к.т.н., доцент кафедры цифровых технологий МГТЭУ
место работы, занимаемая должность

подпись	А.А. Белоглазов И.О. Фамилия	«14» 03 2022 г. Дата

Рабочая программа утверждена на заседании кафедры цифровых технологий
(протокол № 4 от «21» 03 2022 г.)

Декан факультета

«21» 03 2022 г. (дата)	(подпись)	Е.В. Петрунина (Ф.И.О.)

СОГЛАСОВАНО
Начальник
управления по социальной
работе

« » 2022 г. (дата)	(подпись)	(Ф.И.О.)

СОГЛАСОВАНО
Председатель
совета обучающихся

«21» 04 2022 г. (дата)	(подпись)	Коротин Н. (Ф.И.О.)

Содержание

1. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

1.1. Цель и задачи изучения учебной дисциплины (модуля)

Целью изучения дисциплины «Защита в операционных системах» является формирование у студентов знаний по основам использования операционных систем в защищенном исполнении, по средствам и методам обеспечения защиты информации в ОС, а также навыков и умения в применении знаний при проведении работ:
- по разработке и конфигурированию программно-аппаратных средств защиты информации;
- по установке, наладке, тестированию и обслуживанию системного и прикладного программного обеспечения;
- по разработке технических заданий на проектирование, эскизных, технических и рабочих проектов систем и подсистем защиты информации с учетом действующих нормативных и методических документов;
- по подготовке аналитических отчетов по результатам проведенного анализа и выработка предложений по устранению выявленных уязвимостей;
- по установке, наладке, тестированию и обслуживанию программно-аппаратных средств обеспечения информационной безопасности компьютерных систем.
Кроме того, целью дисциплины является развитие в процессе обучения системного мышления, необходимого для решения задач защиты информации с учетом требований системного подхода. Задачи дисциплины – дать знания:
-по концепции построения защищенных ОС;
-по теоретическим основам защиты информации в ОС;
-по возможным угрозам безопасности информации при ее обработке в информационных системах;
-по встроенным в ОС средствам защиты информации;
-по средствам и методам управления доступом в ОС;
-по использованию защищенных ОС в сетях передачи данных.
Требования к результатам освоения дисциплины

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**
ПК-1 Способен использовать и развивать методы научных исследований и инструментария в области проектирования и управления информационными системами в прикладных областях	ПК-1.1 Знает основные подходы, методы в области проектирования и управления информационными системами в прикладных областях; возможности современных инструментальных средств для проектирования и управления информационными системами в прикладных областях; способы представления научно-технической информации.
	ПК-1.2 Умеет использовать и развивать методы научных исследований в области проектирования и управления информационными системами в прикладных областях; анализировать иностранные источники в области проектирования и управления ИС в прикладных областях; использовать и развивать методы инструментарий в области проектирования и управления информационными системами в прикладных областях; правильно подготавливать научно-технические отчеты; оформлять результаты исследований в виде статей и докладов на научных конференциях в предметной области.
	ПК-1.3 Владеет практическими навыками использования и развития инструментальных средств в области проектирования и управления информационными системами в прикладных областях; навыками работы в системах поиска информации,

	текстовых процессорах, электронных таблицах, базах данных и системах подготовки презентаций.
ПК-5 Способен исследовать применение различных научных подходов к автоматизации информационных процессов и информатизации предприятий и организаций	ПК-5.1 Знает различные научные подходы к автоматизации информационных процессов и информатизации предприятий и организаций; процесс подготовки информации к принятию управленческих решений; тенденции развития автоматизации управления промышленными предприятиями.
	ПК-5.2 Умеет провести алгоритмизацию конкретной управленческой задачи; применять различные научные подходы к автоматизации информационных процессов и информатизации предприятий и организаций.
	ПК-5.3 Владеет навыками применения типовых подходов, применяемых при анализе, планировании и оперативном управлении деятельностью промышленного предприятия; навыками исследования применения различных научных подходов к автоматизации информационных процессов и информатизации предприятий и организаций на основе приобретенных знаний и умений и их применения в нетипичных ситуациях.

1.2. Место дисциплины (модуля) в структуре образовательной программы направления подготовки 09.04.03 «Прикладная информатика (уровень магистратуры)»

Учебная дисциплина "Защита в операционных системах" относится к блоку 1 "Дисциплины (модули)" и входит в его базовую часть.

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Объем дисциплины и виды учебной работы в соответствии с формами обучения

Объем дисциплины «Защита в операционных системах» составляет 6 зачетных единиц/216 часов:

Вид учебной работы	Всего, часов	Очная форма	Очная форма	
		Курс, часов	Курс, часов	
		2 курс, 3 сем.	2 курс, 4 сем.	
Аудиторная работа обучающихся с преподавателем (по видам учебных занятий), всего в том числе:	*92*	*32*	*60*	
Лекции	16	8	8	
Практические занятия	40	24	16	
Лабораторные занятия				
Самостоятельная работа обучающихся	124	76	48	
Промежуточная аттестация (подготовка и сдача), всего:				
Контрольная работа	36		36	
Курсовая работа				
Зачет с оценкой	6	3	3	
Экзамен				
Итого: Общая трудоемкость учебной дисциплины (в часах, зачетных единицах)	216\6	108\3	108\3	

2.2. Содержание дисциплины по темам (разделам)

№ п/п	Наименование раздела (темы)	Содержание раздела (тематика занятий)	Формируемые компетенции (индекс)

1.	Понятие защищенной операционной системы. Управление доступом.	Угрозы и классификация наиболее распространенных угроз. Понятие защищенной ОС. Подходы к организации защиты. Этапы построения защиты. Административные методы защиты. Субъекты, объекты, методы и права доступа. Требования к правилам управления доступом. Мандатное управление доступом.	ПК-1,ПК-5
2.	Управление доступом в операционных системах семейства UNIX	Субъекты, объекты, методы и права доступа, UID, EUID, GID, EGID. Средства динамического изменения полномочий субъектов: SUID/SGID.	ПК-1,ПК-5
3	Управление доступом в операционных системах семейства Windows	Субъекты, объекты, методы и права доступа, привилегии субъекта. Порядок проверки прав доступа. Средства динамического изменения полномочий субъектов. мандатный контроль целостности, контроль учетных записей. Элементы изолированной программной среды	ПК-1,ПК-5
4	Идентификация, аутентификация и авторизация	Понятие идентификации, аутентификации и авторизации пользователей. Средства и методы хранения эталонных копий аутентификационной информации. Протоколы аутентификационной информации. Протоколы передачи аутентификационной информации по каналам сети. Криптографическое обеспечение аутентификации пользователей	ПК-1,ПК-5
5	Аутентификация на основе паролей.	Средства и методы защиты от компроментации и подбора паролей. Парольная аутентификаци в UNIX. Парольная аутентификация в Windows. Средства управления параметрами аутентификации	ПК-1,ПК-5
6	Аутентификация на основе внешних носителей ключа	Особенности проверки аутентификационной информации для различных типов носителей ключа. Проблемы рассылки и смены ключей	ПК-1,ПК-5
7	Биометрическая аутентификация	Общая схема, преимущества, проблемы. Достоинства и недостатки различных схем биометрической аутентификации	ПК-1,ПК-5
8	Аудит в операционных системах UNIX и WINDOWS	Необходимость аудита в защищенной системе. Требования к подсистеме аудита ОС.	ПК-1,ПК-5

2.3. Разделы дисциплин и виды занятий

№ п/п	Наименование темы дисциплины	Лекционные занятия	Практические занятия	Самостоятельная работа	Всего часов	Формы текущего контроля успеваемости
1.	Угрозы и классификация наиболее распространенных угроз.	8	20	62	108	Устный опрос
2.	Угрозы в операционных системах UNIX и WINDOWS	8	20	62	108	Устный опрос

Экзамен		6				
	Итого:	16	40	124	216\6	

2.4. Планы теоретических (лекционных) занятий

Тема лекции. Вопросы, отрабатываемые на лекции	**Всего часов**
Требования к защите ОС. Понятие защищенной ОС. Подходы к организации защиты ОС и их недостатки	2
Анализ защищенности современных операционных систем. Встроенные средства защиты Windows, Unix	2
Обзор и статистика методов, лежащих в основе атак на современные ОС	2
Разграничение доступа в ОС. Субъекты, объекты, методы и права доступа. Привилегии субъектов доступа	2
Идентификация и аутентификация пользователей ОС	2
Разграничение доступа к ресурсам в ОС Windows, Unix. Организация разграничения доступа к объектамц	2
Аудит в ОС. Необходимость аудита	2
Защита сетевого взаимодействия Windows, Unix. Методика проникновения. Сбор информации о системе	2

2.5. Планы практических (семинарских) занятий

Тема практического занятия. Вопросы, отрабатываемые на практическом занятии	**Всего часов**
Исследование методов разграничения доступа в ОС Windows. Этапы построения защиты. Административные меры защиты. Управление загрузкой и восстановление данных в Windows	4
Аудит системных процессов и событий в Windows. Анализ выполнения современными ОС формализованных требований к защите информации от НСД..	4
Архивации и восстановления данных в Windows. Классификация атак на ОС и их сравнительная статистика. Шифрование данных в Windows с помощью EFS.	4
Избирательное и полномочное разграничение доступа, изолированная программная среда	4
Аутентификация на основе паролей, методы подбора паролей, средства и методы повышения защищенности ОС от подбора паролей. Аутентификация на основе внешних носителей ключа, биометрических характеристик пользователя	4
Анализ защищенности операционных систем семейства Windows и Unix. Разделяемые сетевые ресурсы, NTFS и права доступа. Распределенная файловая система и права доступа.	4
Требования к подсистеме аудита	4
Защита каналов средствами файервола. Виртуальные частные сети, протоколы	4
Изучение средств защиты сетевого взаимодействия. Настройки зон безопасности. Безопасность приложений с поддержкой сценариев Централизованная настройка приложений через групповые политики. Конфигурирование средств защиты каналов.	4
Применение шаблонов безопасности для защиты рабочих станций пользователей. Защита серверов.	4

2.6. Планы лабораторных работ – не предусмотрено.

Задания, вопросы, для самостоятельного изучения (задания)	**Всего Часов**
Стандарты безопасности ОС	20
Анализ атаки и методов, позволяющих несанкционированно вмешаться в работу ОС	20
Примеры реализации разграничения доступа в современных ОС	20

Примеры реализации идентификации и аутентификации в современных ОС	22
Назначение прав доступа к объектам: файлам и папкам NTFS, сетевым ресурсам, объектам Active Directory	21
Обзор защиты беспроводных сетей	20

3. ОСОБЕННОСТИ ОБУЧЕНИЯ ЛИЦ С ИНВАЛИДНОСТЬЮ И ОВЗ

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться следующих варианты восприятия учебной информации с учетом их индивидуальных психофизических особенностей, в том числе с применением электронного обучения и дистанционных технологий:

1) для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.

2) для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.

3) для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации

4. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение дисциплины для организации самостоятельной работы студентов (содержит перечень основной литературы, дополнительной литературы, программного обеспечения и Интернет-ресурсы).

В распоряжении преподавателей и обучающихся имеется основное необходимое материально-техническое оборудование, Интернет-ресурсы, доступ к полнотекстовым электронным базам, книжный фонд библиотеки Московского государственного гуманитарно-экономического университета.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Перечень основной литературы

1. Проскурин В.Г. Защита в операционных системах. Учебное пособие для вузов. – М.: Издательский центр «Академия», 2012 (план издательства). – 200 с.

2. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: учеб. пособие для студ. высш. учеб. заведений. – М.: Издательский центр «Академия», 2006. – 256с.

3. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов / А.А. Афанасьев, Л.Т. Веденьев, А.А. Воронцов и др.; Под ред. А.А, Шелупанова, С.Л. Груздева, Ю.С. Нахаева. – М.: Горячая линия – Телеком, 2009. – 522 с.

4. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей, М: ИД«Форум». - 2008 г. .- 415 с.

Дополнительная литература

1. Р. Брэгг. Безопасность сетей на основе Microsoft Windows Server 2003. – М.: «Русская редакция». 2006. – 672 с.

2. Х. Майкл, Д. Лебланк. Защищенный код для Windows Vista. – М.: «Русская редакция»,

2008. – 224 с.

3. Р. Моримото, К. Гардиньер, М. Ноэл, О. Драуби. Microsoft Windows Server 2003. Полное руководство. – М.: «Вильямс», 2005. – 1312 с.

4. М. Руссинович, Д. Соломон. Внутреннее устройство Microsoft Windows: Windows 2003

Server, Windows XP, Windows 2000. – СПб: «Русская редакция». 2005. – 992 с.

5. М. Фленов. Linux глазами хакера. – СПб: «БХВ-Петербург». 2006. – 544 с.

6. Проблемы информационной безопасности. Компьютерные системы. – СПб: Издательство Политехнического университета.

Программное обеспечение

Текстовый редактор
Microsoft Windows
Microsoft Office
7-Zip
AcrobatReader

5.2 Электронные ресурсы

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4. Справочно-правовая система «Консультант Плюс» www.consultant.ru
5. Справочно-правовая система «Гарант» » www.garant.ru
6. Федеральный портал «Российское образование www.edu.ru
7. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/
8. Российский биометрический портал www.biometrics.ru
9. Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
10. Сайт Научной электронной библиотеки www.elibrary.ru

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий	Перечень оборудования и технических средств обучения
1.	Лекционная аудитория	Персональный компьютер, мультимедийный проектор
2.	Компьютерный класс	Персональные компьютеры (IBM PC-совместимые) под управлением ОС Microsoft Windows, компьютерная сеть, доступ в сеть Интернет

7. ОЦЕНКА КОМПЕТЕНЦИЙ ПО ИЗУЧАЕМОЙ ДИСЦИПЛИНЕ

№	Критерии оценки			
	«неудовлетворительно»	«удовлетворительно»	«хорошо»	«отлично»

ЗНАТЬ				
1	Студент не усвоил следующие знания: требования к политикам безопасности, требования к установке, наладке и тестированию современных ОС, базовые средства защиты в ОС от несанкционированного доступа к информации (СЗИ НСД ОС)	Студент усвоил основное содержание материала дисциплины, но имеет пробелы в усвоении материала. Имеет несистематизированные знания по темам: требования к политикам безопасности, требования к установке, наладке и тестированию современных ОС	Студент способен самостоятельно выделять главные положения в изученном материале. Знает: требования к политикам безопасности, требования к установке, наладке и тестированию современных ОС,	Студент знает, понимает, выделяет главные положения в изученном материале и Знает: требования к политикам безопасности, требования к установке, наладке и тестированию современных ОС, базовые средства защиты в ОС от несанкционированного доступа к информации (СЗИ НСД ОС)
УМЕТЬ				
2	Студент не умеет формулировать и настраивать политику безопасности основных ОС, настраивать и тестировать ОС, Настраивать СЗИ НСД ОС в соответствии с предъявляемым требованиям по безопасности	Студент испытывает затруднения при настройке политики безопасности основных ОС, создании и модернизации объектов информатизации на базе компьютерных систем в защищенном исполнении.	Студент умеет настраивать политики безопасности основных ОС, создании и модернизации объектов информатизации на базе компьютерных систем в защищенном исполнении. Настраивать СЗИ НСД ОС в соответствии с предъявляемым требованиям по безопасности	Студент умеет самостоятельно настраивать политики безопасности основных ОС, создании и модернизации объектов информатизации на базе компьютерных систем в защищенном исполнении. Настраивать СЗИ НСД ОС в соответствии с предъявляемым требованиям по безопасности обслуживать современне программноаппаратне средста обеспечения информационной безопасности компьютерных систем, включая защищенные

				операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации;
ВЛАДЕТЬ				
3	Студент не владеет навыками разработки формальных моделей политик управления доступом в ОС навыками установки, наладки, тестирования и обслуживания основных ОС	Студент владеет навыками разработки формальных моделей политик управления доступом в ОС	Студент владеет навыками разработки формальных моделей политик управления доступом в ОС навыками установки, наладки, тестирования и обслуживания основных ОС	Студент владеет навыками разработки формальных моделей политик управления доступом в ОС навыками установки, наладки, тестирования и обслуживания основных ОС Средствами настройки СЗИ НСД ОС
	Компетенции или их части не сформированы.	Компетенции или их части сформированы на базовом уровне.	Компетенции или их части сформированы на среднем уровне.	Компетенции или их части сформированы на высоком уровне.

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Интерактивные образовательные технологии, используемые в аудиторных занятиях и самостоятельной работе обучающихся

Семестр	Вид занятия (Л, ПР, ЛР)	Используемые интерактивные образовательные технологии	Количество часов
1	Л	Лекция-беседа, ТСО (мультимедийный проектор, презентации PowerPoint)	16
	ПР	Практикум на ЭВМ, проблемный метод, взаимообучение	40
	ЛР	Не предусмотрены	
	КР	Устный опрос	36

	Сам.работа	ЭБС, дистанционные консультации, взаимообучение в студенческой среде	124
Итого:			216

9. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

9.1. Организация входного, текущего и промежуточного контроля обучения

Входное тестирование – не предусмотрено.

Текущий контроль – устный опрос, защита отчетов по практическим работам, работа на компьютерах в парах, презентация в режиме диалога, работа в парах.

Промежуточная аттестация – зачет с оценкой.

9.2. Тематика рефератов, проектов, творческих заданий, эссе и т.п.

Не предусмотрены.

9.3. Курсовая работа

Не предусмотрено.

9.4. Вопросы к экзамену

1. Unix-подобные системы. ОС Linux.
2. Состав файла. Открытие файла в Unix-подобной системе.
3. Пользователи в Unix-подобной системе. Распределение идентификаторов пользователей. Суперпользователь.
4. Виды доступа в Unix-подобной системе. Особенности прав доступа к файлам и каталогам.
5. Категории пользователей по отношению к файлу в Unix-подобной системе. Варианты записи прав доступа.
6. Эффективные права в Unix-подобной системе. Маска доступа. Аттрибуты файловых систем ext*fs.
7. Жёсткие ссылки в Unix-подобной системе. Символические ссылки.
8. Группы пользователей в Unix-подобной системе. Создание группы. Хранение конфигурации.
9. Управление группами пользователей в Unix-подобной системе. Получение сведений о группах пользователя.
10. Хранение сведений о пользователе в Unix-подобной системе.
11. Механизм sudo в Unix-подобной системе. Хранение конфигурации.
12. Загрузка ОС Linux. Регистрация пользователей.
13. Управление процессами ОС. Виды процессов. Режимы процессов.
14. Идентификаторы процесса в Unix-подобной системе. Приоритет.
15. Наблюдение за процессами в Unix-подобной системе. Переменные окружения. Файловая система /proc.
16. Доступность ресурсов в Unix-подобной системе. Атаки на доступность. Управление службами.
17. Уровень выполнения в ОС Linux. Запуск по расписанию в Unix-подобной системе.
18. Командная оболочка в Unix-подобной системе. Завершение работы в системе.
19. Межпроцессное взаимодействие в Unix-подобной системе. Сигналы. Перенаправление потока. Каналы.
20. Терминальный режим в Unix-подобной системе. Обмен сообщениями.
21. Конфигурация сетевого интерфейса в Unix-подобной системе.
22. Использование протоколов ARP и ICMP в Unix-подобной системе.

23. Исследование сетевого окружения в Unix-подобной системе. Утилиты nmap, tcpdump и aircrack-ng.

24. Конфигурация безпроводного сетевого интерфейса в Unix-подобной системе. Виртуальные интерфейсы.

25. Аудит в Unix-подобной системе: системные журналы и управление протоколированием.

26. Аудит в Unix-подобной системе: уровни значимости и защита системы аудита.

27. Устройства в Unix-подобной системе. Защита устройств. Виртуальные устройства.

28. Монтирование в Unix-подобной системе. Хранение конфигурации.

9.6. Контроль освоения компетенций

Вид контроля	**Контролируемые темы (разделы)**	**Компетенции, компоненты которых контролируются**
Устный опрос	*1-2*	ПК-1,ПК-5

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Номер и дата протокола заседания кафедры	Перечень измененных пунктов	Подпись заведующего кафедрой