МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное
учреждение инклюзивного высшего образования

**«Российский государственный
университет социальных технологий»**

(ФГБОУ ИВО «РГУ СоцТех»)

УТВЕРЖДАЮ

Проректор по образовательной деятельности

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
АРХИТЕКТУРА СЕТЕВОЙ БЕЗОПАСНОСТИ И УПРАВЛЕНИЕ ПРОЦЕССОМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

образовательная программа направления подготовки
09.04.03 «Прикладная информатика»
Б1.В.ДВ.01.02 «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 4

Москва 2024

Содержание

1. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

1.1. Цель и задачи изучения учебной дисциплины (модуля)

Цели:

- формирование у студентов знаний и навыков по вопросам информационной безопасности и защите информации

Задачи:

- Ознакомиться с основами построения защищенных ОИС
- Познакомиться с основными уязвимостями и угрозами информационной безопасности ОИС

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

Дисциплина относится к части учебного плана – «Дисциплины по выбору».

1.3. Требования к результатам освоения дисциплины

Процесс освоения учебной дисциплины направлен на формирование у обучающихся следующих компетенций:
Профессиональные (ПК) – в соответствии с ФГОС 3++.

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
ПК-8 Способен проектировать информационные процессы и системы с использованием инновационных Инструментальныхсредств адаптировать современные ИКТ к задачам прикладных ИС.	ПК-8.1. Знает принципы, методы, положения, определения проектирования информационных процессов и систем с использованием инновационных инструментальных средств; подходы и методы к проектированию информационных процессов и систем, выстраивать архитектуру сетевой безопасности
	ПК-8.2. Умеет разрабатывать, проектировать, тестировать, администрировать информационные процессы и системы с использованием инновационных инструментальных средств; принимать решения по информатизации предприятий и организаций прикладной области в условиях неопределенности и риска; интегрировать компоненты и сервисы информационных систем; проводить моделирование и проектирование информационных систем с учётом обеспечения безопасности
	ПК-8.3. Владеет навыками адаптации современных ИКТ к задачам прикладных ИС на основе приобретенных знаний и умений и их применения в нетипичных ситуациях; практическими навыками проектирования информационных процессов с учетом архитектуры сетевой безопасности; практическими навыками адаптации современных ИКТ к задачам прикладных ИС; навыками выбора технологии проектирования информационных систем

ПК-6 Способен применять современные методы и инструментальные средства прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания ИС	ПК-6.1 Знает различные методы решения задач при создании экономических информационных систем; методы проектирования автоматизированных и информационных систем для решения прикладных задач; информационные технологии, применяемые на этапах разработки, производства, испытаний и эксплуатации продукции с учетом построения архитектуры сетевой безопасности
	ПК-6.2 Умеет осуществлять выбор способа представления информации в соответствии с поставленной задачей; видеть и формулировать проблему информационной безопасности и надежности, ее анализировать, подбирать средства и методы для ее решения и ликвидации; использовать программные средства, применяемые на этапах разработки, производства, испытаний и эксплуатации продукции с учетом построения архитектуры сетевой безопасности
	ПК-6.3 Владеет методами описания информационных систем; навыками сбора, формализации и обработки информации; навыками использования инструментальных средств прикладной информатики создания высоконагруженных информационных систем с учетом построения архитектуры сетевой безопасности; классами, пакетами и возможностями автоматизированных средств обеспечения; навыками работы с информационными технологиями, применяемыми на этапах разработки, производства, испытаний и эксплуатации продукции. Владеет методами управления процессом обеспечения безопасности

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

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

Объем дисциплины «Архитектура сетевой безопасности и управление процессом обеспечения безопасности» составляет 4 зачетных единиц/144 часов:

Вид учебной работы	**Всего, часов**	**Очная форма**
		Курс, часов
	Очная форма	2 курс, 4 семестр
Аудиторная работа обучающихся с преподавателем (по видамучебных занятий), всего в том числе:	40	40
Лекции (Л)	18	18
В том числе, практическая подготовка (ЛПП)		
Практические занятия (ПЗ) ***(в том числе зачет)***	22	22
В том числе, практическая подготовка (ПЗПП)	5	5
Лабораторные работы(ЛР)		

В том числе, практическаяподготовка (ЛРПП)		
Самостоятельная работаобучающихся (СР)	104	104
В том числе, практическаяподготовка (СРПП)	20	20
Промежуточная аттестация (подготовка исдача), всего:		
Контрольная работа		
Курсовая работа		
Зачет	+	+
Экзамен	-	-
Итого: Общая трудоемкость учебной дисциплины (в часах, зачетных единицах)	144/4	144/4

2.2. Содержание дисциплины по темам (разделам)

№ п/п	Наименование раздела(темы)	Содержание раздела (тематика занятий)	Формируемые компетенции (индекс)
1	Сущность, задачи и проблемы информационной безопасности	Термин «высокотехнологический», современные подходы к его пониманию. Инновационный процесскак объект управления. Инновационный процесс: понятие, структура, содержание работ в высокотехнологичных отраслях	ПК-6, ПК-8
2	Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ	Органы, обеспечивающие национальную безопасностьРФ, цели, задачи. Национальные интересы РФ в информационной сфере. Приоритетные направления вобласти защиты информации в РФ.	ПК-6, ПК-8
3	Угрозы информационной безопасности. Управлениерисками.	Понятие угрозы. Виды угроз. Три наиболее выраженные угрозы. а. Характер происхождения угроз: умышленные факторы, естественные факторы. Источники угроз. Предпосылки появления угроз: объективные, субъективные	ПК-6, ПК-8
4	Методы контроля доступа к информации	Математические модели управления доступом к информации. Потоковая модель доступа. Политика безопасности и модель доступа. Способы анализа моделей доступа и политик безопасности. Механизмыразграничения доступа в современных операционных системах. Электронные ключи	ПК-6, ПК-8

2.3. Разделы дисциплины и виды занятий

№п/п	Наименование темы дисциплины	екционные занятия	Практические занятия	Самостоятельная работа	Всего часов	Формы текущего контроля успеваемости
1.	Сущность, задачи и проблемы информационнойбезопасности	4	5	26	35	Устный опрос
2.	Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ	5	5	26	36	Устный опрос
3.	Угрозы информационной безопасности. Управление рисками.	5	6	26	37	Устный опрос
4	Методы контроля доступа к информации	4	6	26	36	Устный опрос
	Зачет					
	Итого:	18	22	104	144\4	

2.4. План самостоятельной работы обучающегося по дисциплине (модулю)

№	Название разделов и тем	Виды самостоятельной работы	Трудоемкость	Формируемые компетенции	Формы контроля
1.	Сущность, задачи и проблемы информационной безопасности	Изучение источников	26	ПК- 6, ПК-8	Устный опрос
2.	Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ	Составление отчетов	26	ПК- 6, ПК-8	Устный опрос
3.	Угрозы информационной безопасности. Управление рисками.	Составление отчетов	26	ПК- 6, ПК-8	Устный опрос
4.	Методы контроля доступа к информации	Составление отчетов	26	ПК- 6, ПК-8	Устный опрос

3. ОСОБЕННОСТИ ОБУЧЕНИЯ ЛИЦ С ИНВАЛИДНОСТЬЮ И ОВЗ

Обучение лиц с ограниченными возможностями здоровья осуществляется с учетом индивидуальных психофизических особенностей, а для инвалидов также в соответствии с индивидуальной программой реабилитации инвалида.

Для получения обучающимися, имеющими ограниченные физические возможности, качественного образования должны выполняться следующие важные условия: обучающийся

должен иметь возможность беспрепятственно посещать образовательное учреждение и использовать в своём обучении дистанционные образовательные технологии.

Для обучения и контроля обучающихся с нарушениями координации движений предусмотрено проведение тестирования с использованием компьютера.

Во время аудиторных занятий обязательно использование средств обеспечения наглядности учебного материала с помощью мультимедийного проектора. Скорость изложения материала должна учитывать ограниченные физические возможности студентов.

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. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2023. — 400 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1912992
2. Криптографическая защита информации : учебное пособие / С.О. Крамаров, О.Ю. Митясова, С.В. Соколов [и др.] ; под ред. С.О. Крамарова. — Москва : РИОР : ИНФРА-М, 2023. — 321 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1716-6. - ISBN 978-5-369-01716-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1899016
3. Ищейнов, В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации : учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. — Москва : ИНФРА-М, 2022. — 256 с. — (Высшее образование: Специалитет). - ISBN 978-5-16-016535-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1861659

5.2 Перечень дополнительной литературы

1. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/537247
2. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2024. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/537000
3. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/544290
4. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2024. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/536132
5. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2024. — 349 с. — (Высшее образование). — ISBN 978-5-534-

02883-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/536902

5.3 Программное обеспечение

Текстовый редактор
Microsoft Windows
Microsoft Office
7-Zip
AcrobatReader

5.4 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. Федеральный портал «Российское образование www.edu.ru
6. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/
7. Российский биометрический портал www.biometrics.ru
8. Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
9. Сайт Научной электронной библиотеки www.elibrary.ru
10. Электронная библиотека «Знаниум»: https://znanium.com
11. Электронная библиотека «Юрайт»: https://urait.ru
12. Электронно-библиотечная система «Лань»: https://e.lanbook.com/

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 знает основные понятия информационной безопасности и кибербезопасности, не имеет представления об архитектуре сетевой безопасности и управлении процессом обеспечения безопасности, не имеет представления о современных информационно-коммуникационных технологиях, используемых в этой сфере	Студент усвоил основное содержание материала дисциплины, но имеет пробелы в усвоении материала. Имеет несистематизированные знания о принципах современных информационно-коммуникационных технологий обеспечения кибербезопасности, о понятиях информационной безопасности, лишь в общих чертах знает о процессах обеспечения безопасности	Студент способен самостоятельно выделять главные положения в изученном материале. Знает принципы современных информационно-коммуникационных технологий обеспечения сетевой безопасности и понимает ее архитектуру, ориентируется в понятиях информационной безопасности и кибербезопасности, имеет представление об основных положениях управления процессом обеспечения безопасности	Студент знает понятия информационной безопасности и кибербезопасности, понимает принципы формирования архитектуры сетевой безопасности, ориентируется в современных информационно-коммуникационных технологиях, используемых в этой сфере, знает особенности управления прцессом обеспечения безопасности
УМЕТЬ				
2	Студент не умеет применять современные методы и информационно-коммуникационные технологии в сфере кибербезопасности; использовать новейшие информационно-коммуникационные технологии в своей профессиональной деятельности. Не умеет описывать и строить архитектуру сетевой безопасности	Студент испытывает затруднения при применении современные методы и информационно-коммуникационные технологии в сфере кибербезопасности; использует информационно-коммуникационные технологии в своей профессиональной деятельности с большими ограничениями (умеет пользоваться основными функциями)	Студент умеет применять современные методы и информационно-коммуникационные технологии в сфере кибербезопасности; использовать базовые функции новейших информационно-коммуникационные технологии в своей профессиональной деятельности, описывать ключевые элементы архитектуры сетевой безопасности и в общем виде осуществлять управление процессом обеспечения безопасности	Студент умеет применять широкий спектр методов и разных ИКТ в сфере кибербезопасности, различать особенности построения различных архитектур сетевой безопасности в разных средах, описывать управление процессом обеспечения безопасности
ВЛАДЕТЬ				
3	Студент не владеет современными технологиями в сфере	Студент испытывает трудности с владением современными	Студент владеет основными технологиями в сфере	Студент хорошо владеет основными технологиями в сфере

	кибербезопасности, не владеет навыками использования современных информационно-коммуникационных технологий в этой сфере, не владеет инструментами выстраивания архитектуры сетевой безопасности и управления процессом обеспечения безопасности	технологиями в сфере кибербезопасности, путается в описании архитектуры сетевой безопасности, плохо владеет навыками использования современных информационно-коммуникационных технологий в этой сфере	кибербезопасности, способен выстраивать и обосновывать архитектуру сетевой безопасности в разных средах, в целом владеет навыками использования современных информационно-коммуникационных технологий в этой сфере, управлением процессом обеспечения безопасности	кибербезопасности, отлично владеет навыками использования современных информационно-коммуникационных технологий при построении архитектуры сеевой безопасности и управлении процессом обеспечения безопасности
	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.

9. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Интерактивные образовательные технологии, используемые в аудиторных занятиях и самостоятельной работе обучающихся – не предусмотрены.

10. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

10.1 Организация входного, текущего и промежуточного контроля обучения

Входное тестирование – не предусмотрено.
Текущий контроль – устный опрос.
Промежуточная аттестация – зачет

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

Не предусмотрены.

10.3 Курсовая работа

Не предусмотрено.

10.4 Вопросы к зачету

1. Аппаратное и программное обеспечение информационной вычислительной системы.
2. Операционная система Windows Server: редакции, лицензирование.
3. Роли и компоненты Windows Server. Платформы виртуализации.
4. Определение и назначение служб каталогов, их основные функции и задачи.
5. Службы каталогов — предвестники Microsoft Active Directory.
6. Ключевые преимущества службы Active Directory.
7. Архитектура Active Directory. Проектирование доменной структуры.
8. Стратегия именования объектов Active Directory.
9. Планирование инфраструктуры DNS и структуры организационных единиц.
10. Служба DHCP.
11. Типы учетных записей.
12. Планирование учетных записей компьютеров.
13. Планирование политики сетевой безопасности. Планирование групп.

14. Планирование групповых политик Active Directory.
15. Наследование групповых политик.
16. Пользовательские групповые политики и групповые политики компьютера.
17. Управление групповыми политиками Active Directory.
18. Удаленная установка программного обеспечения при помощи групповых политик
19. Репликация серверов. Обеспечение отказоустойчивости.
20. Средства защиты информации от несанкционированного доступа. Принцип работы.
21. Основные подсистемы СЗИ от НСД Secret Net Studio. Работа с автономной версией Secret Net Studio.
22. Сетевая версия СЗИ от НСД Secret Net Studio. Интеграция сетевой версии Secret Net Studio в доменную структуру
23. Органы, обеспечивающие национальную безопасностьРФ, цели, задачи.
24. Национальные интересы РФ в информационной сфере.
25. Приоритетные направления вобласти защиты информации в РФ.
26. Понятие угрозы. Виды угроз
27. Понятие угрозы. Характер происхождения угроз: умышленные факторы, естественные факторы.
28. Понятие угрозы. Предпосылки появления угроз: объективные, субъективные
29. Математические модели управления доступом к информации
30. Потоковая модель доступа. Политика безопасности и модель доступа.
31. Механизмы разграничения доступа в современных операционных системах
32. Электронные ключи
33. Ключевые характеристики управления процессом обеспечения безопасности
34. Архитектура сетевой безопасности: определение, принципы построения.
35. Архитектура сетевой безопасности: ключевые характеристики

10.5. Контроль освоения компетенций

Вид контроля	**Контролируемые темы (разделы)**	**Компетенции, компоненты которых контролируются**
Устный опрос	*1,2,3,4*	ПК-6 ,ПК-8

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

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