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)
ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА
ЗАЩИТЫ ИНФОРМАЦИИ

образовательная программа направления подготовки
09.04.03 «Прикладная информатика»
Б1.О.08 «Дисциплины(модули)», Обязательная часть

Профиль подготовки
Прикладная информатика в информационной сфере

Квалификация (степень) выпускника:
Магистр

Форма обучения очная

Курс 2 семестр 3

Москва 2024

Содержание

1.1. Цель и задачи изучения учебной дисциплины (модуля)

Целями освоения учебной дисциплины «Программно-аппаратные средства защиты информации» являются формирование компетенции по основным разделам теоретических и практических основ организации средств защиты информации, дать необходимые навыки по использованию средств защиты информации в компьютерных системах и овладению методами решения соответствующих.

Студенты должны научиться применять современные аппаратно-программные средства защиты информации предоставляемые сетевым оборудованием, являющимся самым уязвимым местом при попытке несанкционированного доступа.

Основными задачами дисциплины являются:

• Ознакомление с основными терминами и определениями.

• Ознакомление с основными типами угроз и атак.

• Изучение механизмов защиты административного интерфейса и разграничения прав доступа.

• Изучение технологии AAA.

• Изучение способов аппаратно-программной защиты сетевых соединений.

• Изучение принципов построения виртуальных частных сетей.

Требования к результатам освоения дисциплины

Код компетенции	Содержание компетенции	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций
ОПК-8	Способен осуществлять эффективное управление разработкой программных средств и проектов	ОК-8.1 Знает архитектуру информационных систем предприятий и организаций; методологии и технологии реинжиниринга, проектирования и аудита прикладных информационных систем различных классов; инструментальные средства поддержки технологии проектирования и аудита информационных систем и сервисов; методы оценки экономической эффективности и качества, управления надежностью и информационной безопасностью; особенности процессного подхода к управлению прикладными ИС; современные ИКТ в процессном управлении; системы управления качеством; концептуальное моделирование процессов управления знаниями; архитектуру систем управления знаниями; онтологии знаний; подсистемы сбора, фильтрации, накопления, доступа, генерации и распространения знаний.

		ОПК-8.2 Умеет выбирать методологию и технологию проектирования информационных систем; обосновывать архитектуру ИС; управлять проектами ИС на всех стадиях жизненного цикла, оценивать эффективность и качество проекта; применять современные методы управления проектами и сервисами ИС; использовать инновационные подходы к проектированию ИС; принимать решения по информатизации предприятий в условиях неопределенности; проводить реинжиниринг прикладных и информационных процессов; обосновывать архитектуру системы управления знаниями.

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

Дисциплина «Программно-аппаратные средства защиты информации» относится к базовой части Блока 1 «Дисциплины (модули)» Для изучения данной дисциплины необходимы знания, умения и навыки по дисциплинам «Техническая защита информации», «Современные технологии разработки программного обеспечения». Освоение данной дисциплины необходимо обучающемуся для изучения дисциплин «Архитектура сетевой безопасности и управление процессом обеспечения безопасности», «Защита в операционных системах», успешного прохождения производственной практики и выполнения выпускной квалификационной работы.

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

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

Объем дисциплины «Программно-аппаратные средства защиты информации» составляет 4 зачетных единиц/144 часов:

Вид учебной работы	Всего, часов	Очная форма
		Курс, часов
		1 курс, 2 сем.
Аудиторная работа обучающихся с преподавателем (по видам учебных занятий), всего в том числе:	*48*	*48*
Лекции	14	14
Практические занятия	34	34
Лабораторные занятия		
Самостоятельная работа обучающихся	96	96
Промежуточная аттестация (подготовка и сдача), всего:		
Контрольная работа		
Курсовая работа		
Зачет с оценкой	+	+
Экзамен		
Итого:	144\4	144\4

Общая трудоемкость учебной дисциплины (в часах, зачетных единицах)		

2.2. Содержание дисциплины по темам (разделам)

№ п/п	Наименование раздела (темы)	Содержание раздела (тематика занятий)	Формируемые компетенции (индекс)
1.	Основные принципы создания и применения программно-аппаратных средств обеспечения информационной безопасности.	Стандарты и спецификации в области ИБ. Задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности.	ОПК-8
2.	Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности, взаимодействие с общесистемными компонентами вычислительных систем	Защита компонентов ПЭВМ. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям. Программно-аппаратные средства шифрования. Применение программно-аппаратного комплекса SecretNet для защиты информации от несанкционированного доступа.	ОПК-8

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.	Основные принципы создания и применения программно-аппаратных средств обеспечения информационной безопасности.	5	12	36	53	Устный опрос
2.	Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности, взаимодействие с общесистемными компонентами вычислительных систем	9	22	60	91	Устный опрос
	Зачет с оценкой				+	
	Итого:	14	34	96	144\4	

2.4. Планы теоретических (лекционных) занятий

Тема лекции. Вопросы, отрабатываемые на лекции	**Всего часов**
Введение. Основные понятия.	2

Стандарты и спецификации в области ИБ. Задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности. Основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности. Категории и модели информационной безопасности	4
Идентификация и аутентификация пользователей. Понятие несанкционированного доступа. Основные подходы к защите данных от НСД	2
Программно-аппаратные средства шифрования. Защита компонентов ПЭВМ. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям. Биометрические средства защиты информации и разграничения доступа	2
Программно-аппаратные средства защиты информации в сетях передачи данных. Аудит безопасности корпоративных систем Обеспечение безопасности доступа к данным информационной системы организации с помощью продуктов Microsoft и Aladdin. Типовые решения. Применение программно-аппаратного комплекса SecretNet для защиты информации от несанкционированного доступа. Построение виртуальных защищенных сетей ViPNet(на платформе Windows). Применение аппаратных ключей Guardant для защиты программного обеспечения от несанкционированного использования.	4

2.5. Планы практических (семинарских) занятий

Тема практического занятия. Вопросы, отрабатываемые на практическом занятии	Всего часов
Обеспечение безопасности доступа к данным информационной системы организации с помощью продуктов Microsoft и Aladdin.	6
Применение программно-аппаратного комплекса SecretNet для защиты информации от несанкционированного доступа.	4
Применение программно-аппаратного комплекса "Соболь" для защиты информации от несанкционированного доступа.	4
Построение виртуальных защищенных сетей ViPNet(на платформе Windows).	6
Применение аппаратных ключей Guardant для защиты программного обеспечения от несанкционированного использования.	6
Программно-аппаратные средства шифрования	8

2.6. Планы лабораторных работ – не предусмотрено.

Задания, вопросы, для самостоятельного изучения (задания)	Всего Часов
Электронная цифровая подпись (ЭЦП)	19
Методы и средства ограничения доступа	22
Средства предотвращения утечки информации по техническим каналам	16
Контроль доступа к файлам	19
Защита от разрушающих программных воздействий (РПВ)	20

3. ОСОБЕННОСТИ ОБУЧЕНИЯ ЛИЦ С ИНВАЛИДНОСТЬЮ И ОВЗ

Для получения учащимися, имеющими ограниченные физические возможности, качественного образования должны выполняться следующие важные условия: учащийся должен иметь возможность беспрепятственно посещать образовательное учреждение и использовать в своём обучении дистанционные образовательные технологии.

Для обучения и контроля учащихся 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. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издатель-ство Юрайт, 2023. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/513300
2. Новожилов, О. П. Информатика в 2 ч. Часть 1 : учебник для вузов / О. П. Новожилов. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 320 с. — (Высшее образование). — ISBN 978-5-534-09964-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/516246
3. Новожилов, О. П. Информатика в 2 ч. Часть 2 : учебник для вузов / О. П. Новожилов. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 302 с. — (Высшее образование). — ISBN 978-5-534-09966-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/516247

5.2 Перечень дополнительной литературы

1. Аппаратные и программные средства защиты информации: Учебное пособие / Душкин А.В., Кольцов А., Кравченко А. - Воронеж:Научная книга, 2016. - 232 с. ISBN 978-5-4446-0746-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/923168– Режим доступа: по подписке.
2. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П.Б. Хорев. — 3-е изд., испр. и доп. — Москва : ИНФРА-М, 2022. — 327 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1035570. - ISBN 978-5-16-015471-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1865598

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
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 усвоил знания о критериях оценки защищенности систем; о проблемах и направлениях развития аппаратных и программных средств защиты информации; о современных криптографических системах; основные стандарты и спецификации в области обеспечения информационной	Студент усвоил основное содержание материала дисциплины, но имеет пробелы в усвоении материала. Имеет несистематизированные знания о критериях оценки защищенности систем; о проблемах и направлениях развития аппаратных и программных средств защиты информации; о современных	Студент способен самостоятельно выделять главные положения в изученном материале. Имеет знания о критериях оценки защищенности систем; о проблемах и направлениях развития аппаратных и программных средств защиты	Студент знает, понимает, выделяет главные положения в изученном материале и способен дать краткую характеристику основным идеям проработанного материала дисциплины. Показывает глубокое знание и понимание : о критериях оценки защищенности

	безопасности; принципы обеспечения информационной безопасности в условиях современного информационного общества возможности использования новых информационных технологий и их средств при практической реализации требований отечественных и международных стандартов информационной безопасности.	криптографических системах; основные стандарты и спецификации в области обеспечения информационной безопасности;	информации; о современных криптографических системах; основные стандарты и спецификации в области обеспечения информационной безопасности;	систем; о проблемах и направлениях развития аппаратных и программных средств защиты информации; о современных криптографических системах; основные стандарты и спецификации в области обеспечения информационной безопасности; принципы обеспечения информационной безопасности в условиях современного информационного общества возможности использования новых информационных технологий и их средств при практической реализации требований отечественных и международных стандартов информационной безопасности.
УМЕТЬ				
2	Студент не умеет использовать методы обеспечения информационной безопасности в работе современной коммерческой организации; создавать условия безотказной эксплуатации программно-аппаратных средств обеспечения	Студент испытывает затруднения при применении методов обеспечения информационной безопасности в работе современной коммерческой организации	Студент умеет применять использовать методы обеспечения информационной безопасности в работе современной коммерческой организации; создавать условия безотказной эксплуатации	Студент умеет применять использовать методы обеспечения информационной безопасности в работе современной коммерческой организации; создавать условия безотказной эксплуатации

	информационной безопасности автоматизированных систем управления коммерческой организацией; обеспечивать конфигурирование безопасных сетевых средств на основе программно-аппаратные средств обеспечения информационной безопасности; определять основные принципы функционирования и обеспечения защиты программно-аппаратных современных средств информационной безопасности.		программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем управления коммерческой организацией; обеспечивать конфигурирование безопасных сетевых средств на основе программно-аппаратные средств обеспечения информационной безопасности; определять основные принципы функционирования и обеспечения защиты программно-аппаратных современных средств информационной безопасности.	программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем управления коммерческой организацией; обеспечивать конфигурирование безопасных сетевых средств на основе программно-аппаратные средств обеспечения информационной безопасности; определять основные принципы функционирования и обеспечения защиты программно-аппаратных современных средств информационной безопасности. - способы использования безопасных информационных технологий в работе современной коммерческой организации; - основные тенденции развития рынка программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем управления организацией; - условия создания и эксплуатации программно-аппаратных средств обеспечения

				информационной безопасности автоматизированных систем управления коммерческой организацией; - безопасные сетевые технологии, в которых используются программно-аппаратные средств обеспечения информационной безопасности; принципы функционирования и обеспечения защиты программно-аппаратных средств информационной безопасности;
ВЛАДЕТЬ				
3	Студент не владеет навыками эффективного использования программно-аппаратные средства обеспечения информационной безопасности информационных технологий в профессиональной деятельности;	Студент владеет навыками эффективного использования программно-аппаратные средства обеспечения информационной безопасности информационных технологий в профессиональной деятельности; ; работы со средствами защиты информации (на основе учебных имитационных программ);	Студент владеет навыками эффективного использования программно-аппаратные средства обеспечения информационной безопасности информационных технологий в профессиональной деятельности; работы со средствами защиты информации (на основе учебных имитационных программ); создавать и эксплуатировать автоматизированные системы, используя программно-аппаратные средства	Студент владеет навыками эффективного использования программно-аппаратные средства обеспечения информационной безопасности информационных технологий в профессиональной деятельности; работы со средствами защиты информации (на основе учебных имитационных программ); создавать и эксплуатировать автоматизированные системы, используя программно-аппаратные средства обеспечения информационной

			обеспечения информационной безопасности АКС в организации;	безопасности АКС в организации; создавать документацию для использования программно-аппаратных средств обеспечения информационной безопасности; применять в различных проектах программно-аппаратные средства обеспечения информационной 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.

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)	14
	ПР	Практикум на ЭВМ, проблемный метод, взаимообучение	34
	ЛР	Не предусмотрены	
	КР	Устный опрос	
	Сам.работа	ЭБС, дистанционные консультации, взаимообучение в студенческой среде	96
Итого:			144

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. Этапы системного анализа.
2. Способы исследования систем
3. Имитационные модели
4. Этапы имитационного моделирования
5. Методы планирования эксперимента на модели
6. Основы планирования многофакторного эксперимента
7. Обработка результатов эксперимента
8. Основные понятия систем массового обслуживания.
9. Классификация СМО
10. Параметры и характеристики систем массового обслуживания
11. Основные методы структурного моделирования
12. Стандарты серии IDEF
13. Методы функционального моделирования
14. Стандарты и спецификации в области ИБ.
15. Задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности.
16. Основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности.
17. Категории и модели информационной безопасности
18. Идентификация и аутентификация пользователей.
19. Понятие несанкционированного доступа. Основные подходы к защите данных от НСД
20. Программно-аппаратные средства шифрования. Защита компонентов ПЭВМ.
21. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.
22. Биометрические средства защиты информации и разграничения доступа
23. Программно-аппаратные средства защиты информации в сетях передачи данных.
24. Аудит безопасности корпоративных систем Обеспечение безопасности доступа к данным информационной системы организации с помощью продуктов Microsoft и Aladdin. Типовые решения.
25. Применение программно-аппаратного комплекса SecretNet для защиты информации от несанкционированного доступа.
26. Построение виртуальных защищенных сетей ViPNet(на платформе Windows).
27. Применение аппаратных ключей Guardant для защиты программного обеспечения от несанкционированного использования.

9.6. Контроль освоения компетенций

Вид контроля	**Контролируемые темы (разделы)**	**Компетенции, компоненты которых контролируются**
Устный опрос	*1-2*	*ОПК-8*

1.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

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