МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Забайкальский государственный университет»
(ФГБОУ ВО «ЗабГУ»)

Энергетический факультет
Кафедра Прикладной информатики и математики

УТВЕРЖДАЮ:

Декан факультета

Энергетический факультет

Батухтин Андрей Геннадьевич

«____»_____20____ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.ДВ.01.01 Защита информации в автоматизированных системах обработки информации и управления
на 108 часа(ов), 3 зачетных(ые) единиц(ы)
для направления подготовки (специальности) 09.04.01 - Информатика и вычислительная техника

составлена в соответствии с ФГОС ВО, утвержденным приказом Министерства образования и науки Российской Федерации от «___» _____ 20____ г. №____

Профиль – Искусственный интеллект в автоматизированных системах обработки информации и управления (для набора 2024)
Форма обучения: Очная

1. Организационно-методический раздел

1.1 Цели и задачи дисциплины (модуля)

Цель изучения дисциплины:

"Защита информации в автоматизированных системах обработки информации и управления" является формирование у студентов глубоких знаний и практических навыков в области обеспечения информационной безопасности, а также разработка и внедрение эффективных мер защиты данных в автоматизированных системах. Это включает в себя понимание современных угроз, методов защиты и правовых аспектов, связанных с безопасностью информации.

Задачи изучения дисциплины:

1.Изучение основ информационной безопасности: ознакомить студентов с ключевыми понятиями, принципами и задачами защиты информации, а также с основными угрозами и уязвимостями, характерными для автоматизированных систем. 2.Анализ угроз и уязвимостей: научить студентов проводить анализ рисков и уязвимостей в автоматизированных системах, включая идентификацию потенциальных угроз и оценку их воздействия на безопасность данных. 3.Разработка мер защиты информации: обучить студентов методам проектирования и внедрения систем защиты информации, включая технические средства (шифрование, антивирусные программы) и организационные меры (политики безопасности, обучение персонала). 4.Управление инцидентами безопасности: подготовить студентов к реагированию на инциденты кибербезопасности, включая выявление, анализ и устранение последствий атак на информационные системы. 5.Использование современных технологий: ознакомить студентов с современными инструментами и технологиями кибербезопасности, такими как системы управления событиями безопасности (SIEM), системы обнаружения вторжений (IDS), а также методы криптографической защиты данных. 6.Правовое регулирование в области защиты информации: изучить законодательство и нормативные акты, регулирующие защиту информации, включая ответственность за нарушение норм безопасности. 7.Формирование компетенций в управлении рисками: научить студентов разрабатывать стратегии управления рисками кибербезопасности, осуществлять мониторинг и контроль за безопасностью автоматизированных систем. 8.Практическое применение знаний: предоставить студентам возможность применять полученные знания на практике через участие в проектах, стажировках или симуляциях инцидентов безопасности.

1.2. Место дисциплины (модуля) в структуре ОП

Дисциплина входит в блок Б1 «Дисциплины (модули)» образовательной программы магистратуры по направлению подготовки 09.04.01 «Информатика и вычислительная техника». Изучение дисциплины предполагает предварительное освоение следующих дисциплин учебного плана: • Технологии разработки программного обеспечения; • Объектно-ориентированное проектирование автоматизированных систем обработки информации и управления. Освоение данной дисциплины необходимо как предшествующее для следующих дисциплин образовательной программы: • Технологии обработки больших данных; • Технологии разработки мультимедиа систем; • Подготовка и защита ВКР. Освоение учебной дисциплины связано с формированием компетенций с учетом матрицы

компетенций ОПОП по направлению подготовки 09.04.01 «Информатика и вычислительная техника».

1.3. Объем дисциплины (модуля) с указанием трудоемкости всех видов учебной работы

Общая трудоемкость дисциплины (модуля) составляет 3 зачетных(ые) единиц(ы), 108 часов.

Виды занятий	Семестр 3	Всего часов
Общая трудоемкость		108
Аудиторные занятия, в т.ч.	51	51
Лекционные (ЛК)	17	17
Практические (семинарские) (ПЗ, СЗ)	0	0
Лабораторные (ЛР)	34	34
Самостоятельная работа студентов (СРС)	57	57
Форма промежуточной аттестации в семестре	Зачет	0
Курсовая работа (курсовой проект) (КР, КП)		

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Планируемые результаты освоения образовательной программы		Планируемые результаты обучения по дисциплине
Код и наименование компетенции	Индикаторы достижения компетенции, формируемые в рамках дисциплины	Дескрипторы: знания, умения, навыки и (или) опыт деятельности
УК-1	УК-1.1.Знать: методы системного и критического анализа методы выявления и решения проблемной ситуации УК-1.2. Уметь: применять методы системного и критического анализа для решения	Знать: методы системного и критического анализа методы выявления и решения проблемной ситуации Уметь: применять методы системного и критического анализа для решения проблемных

	проблемных ситуаций разрабатывать стратегию действий, принимать конкретные решения для ее реализации УК-1.3.Владеть: методологией системного и критического анализа проблемных ситуаций - методиками постановки цели, определения способов ее достижения, разработки стратегий действий	ситуаций разрабатывать стратегию действий, принимать конкретные решения для Владеть: методологией системного и критического анализа проблемных ситуаций - методиками постановки цели, определения способов ее достижения, разработки стратегий действий
УК-2	УК-2.1.Знать: этапы жизненного цикла проекта, его разработки и реализации методы разработки и управления проектами УК-2.2. Уметь: разрабатывать проект, определять целевые этапы, основные направления работ объяснить цели и сформулировать задачи, связанные с подготовкой и реализацией проекта управлять проектом на всех этапах его жизненного цикла, в том числе в нестандартных ситуациях УК-2.3.Владеть: методиками разработки и управления проектом; методами оценки потребности в ресурсах и эффективности проекта, в том числе его экологической и социальной значимости	Знать: этапы жизненного цикла проекта, его разработки и реализации методы разработки и управления проектами Уметь: разрабатывать проект, определять целевые этапы, основные направления работ объяснить цели и сформулировать задачи, связанные с подготовкой и реализацией проекта управлять проектом на всех этапах его жизненного цикла, в том числе в нестандартных ситуациях Владеть: методиками разработки и управления проектом; методами оценки потребности в ресурсах и эффективности проекта, в том числе его экологической и социальной значимости.
УК-4	УК-4.1. Знать: правила и закономерности личной и деловой устной и письменной коммуникации современные	Знать: правила и закономерности личной и деловой устной и письменной коммуникации современные коммуникативные

	коммуникативные технологии на русском и иностранном языках УК-4.2. Уметь: применять на практике коммуникативные технологии, методы и способы делового общения для академического и профессионального взаимодействия УК-4.3.Владеть: методикой межличностного делового общения на русском и иностранном языках, с применением профессиональных языковых форм, средств и современных коммуникативных технологий	технологии на русском и иностранном языках Уметь: применять на практике коммуникативные технологии, методы и способы делового общения для академического и профессионального взаимодействия Владеть: методикой межличностного делового общения на русском и иностранном языках, с применением профессиональных языковых форм, средств и современных коммуникативных технологий
ПК-5	ПК-5.1. Разрабатывает программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях ПК-5.2. Модернизирует программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях	Знать: как разрабатывать программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях Уметь: модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях

3. Содержание дисциплины

3.1. Разделы дисциплины и виды занятий

3.1 Структура дисциплины для очной формы обучения

Модуль	Номер раздела	Наименование раздела	Темы раздела	Всего часов	Аудиторные занятия			СРС
					ЛК	ПЗ (СЗ)	ЛР	
1	1.1	Основы информационной безопасности АСОИУ	Тема 1,2,3,4	108	17	0	34	57
	1.2	Методы, стандарты и задачи ИИ информационной безопасности АСОИУ	Тема 5,6,7,8,9	57	10	0	17	30
Итого				165	27	0	51	87

3.2. Содержание разделов дисциплины

3.2.1. Лекционные занятия, содержание и объем в часах

Модуль	Номер раздела	Тема	Содержание	Трудоемкость (в часах)
1	1.1	Тема 1,2,3,4	Информационная безопасность компьютерных систем и проблемы искусственного интеллекта (ИИ) в информационной безопасности АСОИУ. Основные понятия и определения. Основные угрозы безопасности АСОИУ. Обеспечение безопасности АСОИУ. Принципы криптографической защиты информации. Аппаратнопрограммные средства защиты компьютерной информации. Экспертные системы и базы знаний	7

				по информационной безопасности. SGRC-платформы как основа решения задач ИИ информационной безопасности АСОИУ.Классические симметричные криптосистемы. Основные понятия и определения. Шифры перестановки. Шифрующие таблицы. Применение магических квадратов. Шифры простой замены. Система шифрования Цезаря. Аффинная система подстановок Цезаря. Система Цезаря с ключевым словом. Одноразовая система шифрования. Шифрование методом гаммирования. Методы генерации псевдослучайных последовательностей чисел. Современные симметричные криптосистемы. Американский стандарт шифрования данных DES. Основные режимы работы алгоритма DES. Режим "Электронная кодовая книга". Режим "Сцепление блоков шифра". Режим "Обратная связь по шифру". Режим "Обратная связь по выходу". Области применения алгоритма DES . Комбинирование блочных алгоритмов. Алгоритм шифрования данных IDEA. Отечественный стандарт шифрования данных. Режим простой замены. Режим гаммирования. Режим гаммирования с обратной связью. Режим выработки имитовставки. Блочные и поточные шифры. Криптосистема с депонированием ключа. Процедура генерации ключей. Обслуживание ключей. Процедура дешифрования. Асимметричные криптосистемы. Концепция криптосистемы с открытым ключом. Однонаправленные функции. Криптосистема шифрования данных RSA. Процедуры шифрования и расшифрования в криптосистеме RSA. Безопасность и быстродействие криптосистемы RSA. Схема шифрования Полига – Хеллмана. Схема шифрования Эль Гамаля.	

			Комбинированный метод шифрования.	
	1.2	Тема 5,6,7,8,9	Управление криптографическими ключами. Генерация ключей. Хранение ключей. Носители ключевой информации. Концепция иерархии ключей. Распределение ключей. Распределение ключей с участием центра распределения ключей. Прямой обмен ключами между пользователями. Методы и средства защиты от удаленных атак через сеть Internet. Задачи ИИ решаемые SGRC платформой EGIDA. Особенности функционирования межсетевых экранов. Основные компоненты межсетевых экранов. Фильтрующие маршрутизаторы. Шлюзы сетевого уровня. Шлюзы прикладного уровня. Усиленная аутентификация. Основные схемы сетевой защиты на базе межсетевых экранов. Межсетевой экран - фильтрующий маршрутизатор. Межсетевой экран на основе двупортового шлюза. Межсетевой экран на основе экранированного шлюза. Межсетевой экран - экранированная подсеть. Применение межсетевых экранов для организации виртуальных корпоративных сетей. Программные методы защиты. EGIDA современная интеллектуальная SGRC- платформа для решения задач ИИ информационной безопасности АСОИУ	10

3.2.2. Практические занятия, содержание и объем в часах

Модуль	Номер раздела	Тема	Содержание	Трудоемкость (в часах)

3.2.3. Лабораторные занятия, содержание и объем в часах

Модуль	Номер раздела	Тема	Содержание	Трудоемкость (в часах)
1	1.1	Тема 1,2,3,4	Основные понятия и определения в области информационной безопасности. SGRC-платформы как основа решения задач ИИ информационной безопасности АСОИУ. Основы Российского законодательства в области защиты информации. Регуляторы в области информационной безопасности. Аудит соответствия требованиям Российского законодательства в области защиты информации кредитных организаций. Аудит соответствия требованиям Российского законодательства в области защиты персональных данных. Классические симметричные криптосистемы. Современные симметричные криптосистемы. Асимметричные криптосистемы.	17
	1.2	Тема 5,6,7,8,9	Управление криптографическими ключами. Многофакторные и биометрические системы аутентификации. EGIDA современная интеллектуальная SGRC- платформа. Современные стандарты и спецификации по информационной безопасности. Стандарт безопасности Банка России СТО БР. Стандарт PCI DSS. Стандарт безопасности индустрии платежных карт. Стандарт Общие Критерии (ОК) ISO/IEC 15408 "Критерии оценки безопасности информационных технологий"	17

3.3. Содержание материалов, выносимых на самостоятельное изучение

Модуль	Номер раздела	Содержание материалов, выносимого на самостоятельное изучение	Виды самостоятельной деятельности	Трудоемкость (в часах)
1	1.1	Информационная безопасность	Проработка учебного материала лекций.	27

		компьютерных систем и проблемы искусственного интеллекта (ИИ) в информационной безопасности АСОИУ. Основные понятия и определения. Основные угрозы безопасности АСОИУ. Обеспечение безопасности АСОИУ. Принципы криптографической защиты информации. Аппаратнопрограммные средства защиты компьютерной информации. Экспертные системы и базы знаний по информационной безопасности. SGRC-платформы как основа решения задач ИИ информационной безопасности АСОИУ.Классические симметричные криптосистемы. Основные понятия и определения. Шифры перестановки. Шифрующие таблицы. Применение магических квадратов. Шифры простой замены. Система шифрования Цезаря. Аффинная система подстановок Цезаря. Система Цезаря с ключевым словом. Одноразовая система шифрования. Шифрование методом гаммирования. Методы генерации псевдослучайных последовательностей чисел. Современные симметричные	Выполнение домашнего задания. Другие виды самостоятельной работы.	

		криптосистемы. Американский стандарт шифрования данных DES. Основные режимы работы алгоритма DES. Режим "Электронная кодовая книга". Режим "Сцепление блоков шифра". Режим "Обратная связь по шифру". Режим "Обратная связь по выходу". Области применения алгоритма DES . Комбинирование блочных алгоритмов. Алгоритм шифрования данных IDEA. Отечественный стандарт шифрования данных. Режим простой замены. Режим гаммирования. Режим гаммирования с обратной связью. Режим выработки имитовставки. Блочные и поточные шифры. Криптосистема с депонированием ключа. Процедура генерации ключей. Обслуживание ключей. Процедура дешифрования. Асимметричные криптосистемы. Концепция криптосистемы с открытым ключом. Однонаправленные функции. Криптосистема шифрования данных RSA. Процедуры шифрования и расшифрования в криптосистеме RSA. Безопасность и быстродействие криптосистемы RSA. Схема шифрования Полига – Хеллмана.		

		Схема шифрования Эль Гамаля. Комбинированный метод шифрования.		
	1.2	Управление криптографическими ключами. Генерация ключей. Хранение ключей. Носители ключевой информации. Концепция иерархии ключей. Распределение ключей. Распределение ключей с участием центра распределения ключей. Прямой обмен ключами между пользователями. Методы и средства защиты от удаленных атак через сеть Internet. Задачи ИИ решаемые SGRC платформой EGIDA. Особенности функционирования межсетевых экранов. Основные компоненты межсетевых экранов. Фильтрующие маршрутизаторы. Шлюзы сетевого уровня. Шлюзы прикладного уровня. Усиленная аутентификация. Основные схемы сетевой защиты на базе межсетевых экранов. Межсетевой экран - фильтрующий маршрутизатор. Межсетевой экран на основе двупортового шлюза. Межсетевой экран на основе экранированного шлюза. Межсетевой экран - экранированная подсеть. Применение межсетевых	Проработка учебного материала лекций. Выполнение домашнего задания. Другие виды самостоятельной работы.	30

		экранов для организации виртуальных корпоративных сетей. Программные методы защиты. EGIDA современная интеллектуальная SGRC-платформа для решения задач ИИ информационной безопасности АСОИУ		

4. Фонд оценочных средств для проведения текущей и промежуточной аттестации обучающихся по дисциплине

Фонд оценочных средств текущего контроля и промежуточной аттестации по итогам освоения дисциплины представлен в приложении.

Фонд оценочных средств

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Основная литература

5.1.1. Печатные издания

1. Бондарев В.В. Введение в информационную безопасность автоматизированных систем: учебное пособие / Бондарев В.В.- 2-е изд.- М.: Изд-во МГТУ им. Н. Э. Баумана, 2018. - 250 с.: ил. – 2. Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. Семь безопасных информационных технологий/ под ред. А.С. Маркова. – М.: ДМК Пресс, 2017. -224 с.: ил.

5.1.2. Издания из ЭБС

1.

5.2. Дополнительная литература

5.2.1. Печатные издания

1. Ю.В. Романец и др. Защита информации в компьютерных системах и сетях Изд. 2-е., М:Радио и связь, 2001-376с. 4. Б. Шнаер Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си.-М.:ТРИУМФ, 2003-816с. 5. Математические и компьютерные основы криптологии: Учеб. пособие/Ю.С.Харин и др.-Минск:Новое Знание, 2003-382с. 6. Исагулиев К.П. Справочник по криптологии. Минск:Новое знание, 2004 - 237с

5.2.2. Издания из ЭБС

1. 1. Сайт библиотеки МГТУ им. Н.Э. Баумана: http://library.bmstu.ru. 2.Сайт

вебконсорциума: https://www.w3.org/ 3. ISO/IEC 12207:2008: Информационные технологии. Процессы жизненного цикла программного обеспечения: http://www.iso.org/iso/ru/catalogue_detail?csnumber=43447; 4. ГОСТ Р ИСО/МЭК 15288 – 2005: Системная инженерия. http://www.novsu.ru/file/977849; 5. Capability Maturity Model Integration (CMMI). - http://habrahabr.ru/post/79130/.

5.3. Базы данных, информационно-справочные и поисковые системы

Название	Ссылка

6. Перечень программного обеспечения

Программное обеспечение общего назначения: ОС Microsoft Windows, Microsoft Office, ABBYY FineReader, ESET NOD32 Smart Security Business Edition, Foxit Reader, АИБС "МегаПро".

Программное обеспечение специального назначения:

1) LibreOffice

7. Материально-техническое обеспечение дисциплины

Наименование помещений для проведения учебных занятий и для самостоятельной работы обучающихся	Оснащенность специальных помещений и помещений для самостоятельной работы
Учебные аудитории для проведения занятий лекционного типа	Состав оборудования и технических средств обучения указан в паспорте аудитории, закрепленной расписанием по факультету
Учебные аудитории для проведения лабораторных занятий	
Учебные аудитории для промежуточной аттестации	
Учебные аудитории для проведения групповых и индивидуальных консультаций	Состав оборудования и технических средств обучения указан в паспорте аудитории, закрепленной расписанием по кафедре
Учебные аудитории для текущей аттестации	

8. Методические рекомендации по организации изучения дисциплины

Приступая к работе, каждый студент должен принимать во внимание следующие положения.
Дисциплина построена по модульному принципу, каждый модуль представляет собой логически завершенный раздел курса. Дисциплина делится на два модуля.
На первом занятии каждый студент получает в электронном виде полный комплекс учебно-методических материалов по дисциплине.
Лекционные занятия посвящены рассмотрению ключевых, базовых положений курса и

разъяснению учебных заданий, выносимых на самостоятельную проработку.
Лабораторные работы предназначены для приобретения опыта практической реализации основной профессиональной образовательной программы. Указания к лабораторным работам прорабатываются студентами во время самостоятельной подготовки. Необходимый уровень подготовки контролируется перед проведением лабораторных работ.
Самостоятельная работа студентов включает проработку материала лекций, подготовку к лабораторным работам, подготовку к рубежным контролям.
Текущий контроль проводится в течение каждого модуля, его итоговые результаты складываются из оценок по следующими видам контрольных мероприятий:
-рубежные контроли;
-контроль текущих знаний;
-посещение лекций.
Освоение дисциплины, ее успешное завершение на стадии промежуточной аттестации возможно только при регулярной работе во время семестра и планомерном прохождении текущего контроля.
Для завершения работы в семестре студент должен выполнить все контрольные мероприятия.
Промежуточная аттестация по результатам семестра по дисциплине проходит в форме зачета. Для ликвидации академической задолженности, или перезачета дисциплины для студентов, переводящихся из других вузов, или для повышения балльной оценки за отдельные модули дисциплины проводится зачет в форме собеседования для проверки ключевых результатов обучения по дисциплине, обеспечивающее возможность объективной независимой оценки приобретенных знаний, умений и навыков.

Разработчик/группа разработчиков:
Ксения Валерьевна Беломестнова

Типовая программа утверждена

Согласована с выпускающей кафедрой
Заведующий кафедрой
_____ «___»_____20____г.