ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Руководитель направления

ЮУрГУ
Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Захарова Ю. А.
Пользователь: zakharovaya
Дата подписания: 31.08.2026

Ю. А. Захарова

РАБОЧАЯ ПРОГРАММА

дисциплины 1.О.20 Защита информации и кибербезопасность
для направления 09.03.01 Информатика и вычислительная техника
уровень Бакалавриат
форма обучения заочная
кафедра-разработчик Гуманитарные, естественно-научные и технические дисциплины

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 09.03.01 Информатика и вычислительная техника, утверждённым приказом Минобрнауки от 19.09.2017 № 929

Зав.кафедрой разработчика,
к.юрид.н., доц.

ЮУрГУ
Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Салимгареева А. Р.
Пользователь: salimgareevaar
Дата подписания: 15.07.2026

А. Р. Салимгареева

Разработчик программы,
старший преподаватель

ЮУрГУ
Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Буйлушкина Л. Н.
Пользователь: builushkinaln
Дата подписания: 15.07.2026

Л. Н. Буйлушкина

Нижневартовск

1. Цели и задачи дисциплины

Целью дисциплины «Защита информации и кибербезопасность» является: - изучение основных направлений защиты компьютерной информации; - изучение организационных и административных методов защиты информации; - изучение программно-аппаратных средств защиты компьютерных систем; - обзор готовых решений по обеспечению информационной безопасности, разработка программных средств аудита безопасности, выявления вторжений и программных средств криптографической защиты информации. Задачами дисциплины являются: - дать знания студентам по основным угрозам безопасности компьютерных систем; - дать знания основных стандартов безопасности компьютерных систем; - дать знания моделей безопасности компьютерных систем; - дать знания основных криптографических систем; - дать знания основ администрирования сетей и защиты информации в сетях.

Краткое содержание дисциплины

Основы информационной безопасности и защита информации. История криптографии. Основные термины и определения. Классификация шифров. Шифры замены. Шифры перестановки. Шифры гаммирования. Комбинированные шифры. Шифрование с открытым ключом. Хеш-функции. Криптографические протоколы. протоколы обмена ключами. Протоколы аутентификации (идентификации). Протоколы электронной цифровой подписи. Протоколы контроля целостности. Протоколы электронных платежей. Протоколы голосования. Другие протоколы. Некоторые сведения из теорий алгоритмов и чисел. Основы криптоанализа. Стеганография. Кодирование информации.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Знает: основные нормативные правовые акты в области обеспечения защиты информации и кибербезопасности. Умеет: применять действующую законодательную базу в области обеспечения защиты информации и кибербезопасности. Имеет практический опыт: владения профессиональной терминологией в области информационной безопасности, с учетом ее основных требований.
ОПК-4 Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	Знает: структуру документов и нормативные требования к их составлению в области защита информации и кибербезопасности. Умеет: разрабатывать технические задания на создание подсистем защита информации и кибербезопасности. Имеет практический опыт: работы с документами в области защита информации и кибербезопасности.

ПК-3 Способен анализировать требования к компонентам аппаратно-программных комплексов и программному обеспечению	Знает: основы организационной защита информации при работе с компонентами аппаратно-программных комплексов и программным обеспечением. Умеет: анализировать требования к компонентам аппаратно-программных комплексов и программному обеспечению и выполнять защиту информации на физическом и программном уровнях. Имеет практический опыт: методами организации защиты информации на физическом и программных уровнях.

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
1.О.08 Основы теории булевых функций, 1.Ф.02 Нейросетевые технологии и интеллектуальный анализ, 1.О.21 Компьютерные сети, 1.О.26 Формализация информационных представлений и преобразований, 1.Ф.03 Компьютерное зрение, 1.Ф.08 Анализ данных, моделирование и методы искусственного интеллекта, Производственная практика (научно-исследовательская работа) (8 семестр)	Не предусмотрены

Требования к «входным» знаниям, умениям, навыкам студента, необходимым при освоении данной дисциплины и приобретенным в результате освоения предшествующих дисциплин:

Дисциплина	Требования
1.О.08 Основы теории булевых функций	Знает: теоретические основы и понятийный аппарат алгебры логики; формы представления логических функций. Умеет: анализировать и исследовать логические формулы; строить таблицы истинности; проводить тождественные преобразования логических формул на основе законов алгебрылогики; переводить логические функции в заданный базис; минимизировать логические функции. Имеет практический опыт: применения карт Карно для минимизации булевых функций.
1.Ф.08 Анализ данных, моделирование и методы искусственного интеллекта	Знает: основные концепции, архитектуры и методы искусственного интеллекта (ИИ) и машинного обучения (ML);способы математического и имитационного моделирования систем;алгоритмы классификации, кластеризации и регрессионного анализа;архитектуры искусственных нейронных сетей, многослойные сети, рекуррентные. Умеет: разрабатывать, обучать и тестировать

	математические модели в специализированных программных средах;выбирать оптимальные алгоритмы машинного обучения для классификации или прогнозирования. Имеет практический опыт: инструментарием для визуализации данных и оценки метрик качества моделей;технологиями обработки и анализа данных в условиях неопределенности;использования методов разработки интеллектуальных информационных систем.
1.О.26 Формализация информационных представлений и преобразований	Знает: языки формализации функциональных спецификаций; методы формального представления информационных объектов и процессов, способы их параметризации с применением дискретной математики. Умеет: адекватно использовать и обосновывать применяемые методы формального представления информационных объектов и процессов и способы их параметризации, применяя математический аппарат дискретной математики. Имеет практический опыт: разработки формального описания информационных объектов используя математический аппарат дискретной математики.
1.О.21 Компьютерные сети	Знает: общие характеристики коммутационного оборудования; принципы планирования и документирования локальных вычислительных сетей., принципы установки и конфигурирования коммутационного оборудования; интерфейс командной строки на коммутационном оборудовании; методы диагностики сетей и поиска неисправностей., характеристики сетевого оборудования и принципы его установки и подключения;принципы работы CLI сетевого оборудования различных вендоров; характеристики коммутационных кабелей и принципы их прокладки; методы инсталляции сетевого программного обеспечения на сетевое оборудование и персональные компьютеры. Умеет: планировать сеть на основе требований предъявляемых к сети и технической документации оборудования; планировать обновление сети на основе растущих требований к вычислительной сети., использовать CLI и веб интерфейс для конфигурирования оборудования; проводить подключение конечных узлов и сетевого оборудования к локальной сети; обнаруживать неисправность в локальной вычислительной сети., создавать и настраивать локальную сеть согласно техническим требованиям; подбирать оптимальную конфигурацию сетевого оборудования для сетей различной сложности на основе характеристик сетевого оборудования;проводить настройку персонального компьютера и сетевого

	оборудования для работы в локальной сети; инсталлировать сетевое программное обеспечение на персональный компьютер и сетевое оборудование. Имеет практический опыт: планирования, обновления и документирования сети малого предприятия., работы коммутационными шкафами; работы с инструментами для обжима и заделки кабеля типа "витая пара", обжима и укладки коммутационного кабеля, монтажа локальнойсети; построения локальной вычислительной сети второго и третьего уровня; работы с оборудованием для монтажа коммутационных кабелей; работы с оборудованием для поиска неисправностей на коммутационных линиях., обновления/восстановления/резервного копирования программного обеспечения сетевого оборудования.
1.Ф.03 Компьютерное зрение	Знает: основные принципы формирования цифровых изображений и методы их обработки;архитектуры современных нейронных сетей;базовые алгоритмы: фильтрация, выделение контуров, сегментация, методы поиска и распознавания объектов. Умеет: проектировать и разрабатывать алгоритмы цифровой обработки изображений и видеопотока;выполнять оценку производительности алгоритмов и точность распознавания объектов. Имеет практический опыт: использования инструментальных средств разработки систем искусственного интеллекта и компьютерного зрения;навыка получения полезной информации (аналитики) на основе анализа изображений.
1.Ф.02 Нейросетевые технологии и интеллектуальный анализ	Знает: теоретические основы искусственного интеллекта, машинного обучения и нейросетевых архитектур;классификацию методов интеллектуального анализа данных, включая алгоритмы кластеризации, классификации, регрессии и снижения размерности. Умеет: проводить предварительную подготовку, очистку и нормализацию сырых данных перед их подачей в нейросеть;обучать нейросети, настраивать гиперпараметры и оценивать качество моделей с помощью метрик;визуализировать данные и результаты работы алгоритмов интеллектуального анализа. Имеет практический опыт: использования инструментария для создания, компиляции и обучения нейронных сетей в специализированных программных средах;использования методологии оценки переобучения моделей, а также методов повышения их обобщающей способности;навыка решения типовых прикладных задач с

	использованием нейросетей (распознавание образов, прогнозирование).
Производственная практика (научно-исследовательская работа) (8 семестр)	Знает: требования к компонентам аппаратно-программных комплексов и программному обеспечению; возможности типовой информационной системы. Умеет: анализировать требования к компонентам аппаратно-программных комплексов и программному обеспечению; выявлять первоначальные требования к информационной системе;определять возможности достижения соответствия информационной системы первоначальным требованиям. Имеет практический опыт: информирования заказчика о возможностях типовой информационной системы и вариантах ее модификации; проводить презентации.

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 3 з.е., 108 ч., 10,5 ч. контактной работы с применением дистанционных образовательных технологий

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		10
Общая трудоёмкость дисциплины	108	108
Аудиторные занятия:	4	4
Лекции (Л)	0	0
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	4	4
Лабораторные работы (ЛР)	0	0
Самостоятельная работа (СРС)	97,5	97,5
Подготовка реферата, презентации	40	40
подготовка к занятиям, изучение лекционного материала на портале	37,5	37.5
Подготовка к зачету	20	20
Консультации и промежуточная аттестация	6,5	6,5
Вид контроля (зачет, диф.зачет, экзамен)	-	диф.зачет

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Основы информационной безопасности и защита информации.	0	0	0	0
2	История криптографии. Основные термины и определения. Классификация шифров	0	0	0	0
3	Шифры замены. Шифры перестановки. Шифры гаммирования.	2	0	2	0

	Комбинированные шифры. Шифрование с открытым ключом. Хеш-функции.				
4	Криптографические протоколы. протоколы обмена ключами. Протоколы аутентификации (идентификации). Протоколы электронной цифровой подписи.	1	0	1	0
5	Протоколы контроля целостности. Протоколы электронных платежей. Протоколы голосования. Другие протоколы.	1	0	1	0
6	Некоторые сведения из теорий алгоритмов и чисел. Основы криптоанализа. Стеганография. Кодирование информации.	0	0	0	0

5.1. Лекции

Не предусмотрены

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	3	Шифры замены: Основы шифрования, шифры: однозначной замены, полиалфавитные, омофонические, полиалфавитные. Шифры перестановки: Основы шифрования, шифры одинарной и множественной перестановки. Шифры гаммирования: Основы шифрования, шифрование по модулю N и 2, генерация гаммы, генераторы гамм. Комбинированные шифры: Основы шифрования, ADFGX, DES, ГОСТ 28147-89. Шифрование с открытым ключом: Основы шифрования, алгоритм RSA, алгоритм на основе задачи об укладке ранца, вероятностное шифрование, алгоритм шифрования Эль-Гамаля, алгоритм на основе эллиптических кривых.	2
2	4	Криптографические протоколы. протоколы обмена ключами: Основные сведения о криптографических протоколах, протоколы обмена ключами. Протоколы аутентификации (идентификации): Общие сведения, парольная идентификация / аутентификация, протокол идентификации / аутентификации с использованием хеш-функции, протокол идентификации / аутентификации на основе шифрования с открытым ключом, сервер аутентификации Kerberos, идентификация / аутентификация с помощью биометрических данных, идентификационные карты (ID-cards) и электронные ключи. Протоколы электронной цифровой подписи: Общие сведения, протокол на базе алгоритма RSA, алгоритм цифровой подписи ГОСТ 34.10-94, алгоритм цифровой подписи ГОСТ 34.10-2001, разновидности ЭЦП.	1
2	5	Протоколы контроля целостности: Общие сведения, использование контрольных сумм, использование ЭЦП, использование MAC-кодов, проверка четности, использование ECC, комбинированные методы. Протоколы электронных платежей: Общие сведения, пластиковые карты, суррогатные платежные средства в Internet, расчеты пластиковыми карточками в Internet, электронные кошелки в Internet, цифровые деньги. Протоколы голосования: Общие сведения, некоторые варианты реализации протоколов электронного голосования, российский опыт электронного голосования. Другие протоколы: Протокол разделения секрета, протокол подбрасывания монеты "по телефону", тайные многосторонние вычисления.	1

5.3. Лабораторные работы

Не предусмотрены

5.4. Самостоятельная работа студента

Выполнение СРС			
Подвид СРС	Список литературы (с указанием разделов, глав, страниц) / ссылка на ресурс	Семестр	Кол-во часов
Подготовка реферата, презентации	ЭУМД ОСН. 1 стр. 25-65; стр. 75-87; стр. 111-130; стр. 93-101; стр. 183-210; ЭУМД доп. 1 стр. 41-95; стр. 131-148 Защита информации и криптография: методические указания по выполнению самостоятельной работы для обучающихся по направлению 09.03.04 Программная инженерия / Л.Н.Буйлушкина – Нижневартовск, 2021. – 9 с.	10	40
подготовка к занятиям, изучение лекционного материала на портале	ЭУМД ОСН. 1 стр. 25-65; стр. 75-87; стр. 111-130; стр. 93-101; стр. 183-210; ЭУМД осн. 2 стр. 7-14; стр. 15-39 ЭУМД доп. 1 стр. 41-51;	10	37,5
Подготовка к зачету	ЭУМД ОСН. 1 стр. 25-65; стр. 75-87; стр. 111-130; стр. 93-101; стр. 183-210; ЭУМД осн. 2 стр. 7-14; стр. 15-39 ЭУМД доп. 1 стр. 41-51;	10	20

6. Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации

Контроль качества освоения образовательной программы осуществляется в соответствии с Положением о балльно-рейтинговой системе оценивания результатов учебной деятельности обучающихся.

6.1. Контрольные мероприятия (КМ)

№ КМ	Се-местр	Вид контроля	Название контрольного мероприятия	Вес	Макс. балл	Порядок начисления баллов	Учи-тыва-ется в ПА
1	10	Текущий контроль	Шифрование, дешифрование информации с применением комбинированных криптографических алгоритмов	1	15	13-15 баллов - практические навыки работы с освоенным материалом полностью сформированы 11-13 баллов - практические навыки работы с освоенным материалом сформированы недостаточно 9-11 баллов - необходимые практические навыки работы с освоенным материалом в основном сформированы	зачет
2	10	Текущий контроль	Режимы работы блочных шифров. Схемы кратного шифрования	1	15	13-15 баллов - практические навыки работы с освоенным материалом полностью сформированы 11- 13 баллов - практические навыки работы с освоенным материалом	зачет

						сформированы недостаточно 9-11 баллов - необходимые практические навыки работы с освоенным материалом в основном сформированы	
3	10	Текущий контроль	Дешифрование заданной фразы с применением известного криптографического алгоритма	1	15	13-15 баллов - практические навыки работы с освоенным материалом полностью сформированы 11-13 баллов - практические навыки работы с освоенным материалом сформированы недостаточно 9-11 баллов - необходимые практические навыки работы с освоенным материалом в основном сформированы	зачет
4	10	Текущий контроль	Программная реализация криптографических протоколов	1	15	13-15 баллов - практические навыки работы с освоенным материалом полностью сформированы 11-13 баллов - практические навыки работы с освоенным материалом сформированы недостаточно 9-11 баллов - необходимые практические навыки работы с освоенным материалом в основном сформированы	зачет
5	10	Проме-жуточная аттестация	Зачет	-	30	студенты в аудитории индивидуально отвечают на теоретические вопросы, которые включают вопросы по пройденным разделам, преподаватель беседует и оценивает. 17-30 баллов оценка Зачтено: знает основной материал дисциплины; верно излагает и интерпретирует знания; изложение материала логически выстроено. Меньше 17 баллов оценка Не зачтено: не знает значительной части материала дисциплины; ответ не дан или допускает грубые ошибки при изложении ответа на вопрос; неверно излагает и интерпретирует знания; изложение материала логически не выстроено.	зачет

6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
зачет	Зачет включает в себя теоретическую и практическую части. Теоретическая часть выполняется в виде ответа на вопросы. Практическое часть состоит из выполненных в течении семестра практических работ. Для расчета итоговой оценки баллы за ответы на теоретические вопросы и практические работы представляются в виде доли от максимального балла конкретного задания и ответа на вопрос, выраженной в	В соответствии с пп. 2.5, 2.6 Положения

	процентах. Итоговая оценка за семестр определяется как среднее арифметическое оценок за задания. Зачтено: Итоговая оценка в диапазоне 61 - 100% . Не зачтено: Итоговая оценка в диапазоне 0 -60% .	

6.3. Паспорт фонда оценочных средств

Компетенции	Результаты обучения	№ КМ				
		1	2	3	4	5
ОПК-3	Знает: основные нормативные правовые акты в области обеспечения защиты информации и кибербезопасности.	+	+	+	+	+
ОПК-3	Умеет: применять действующую законодательную базу в области обеспечения защиты информации и кибербезопасности.	+	+	+	+	+
ОПК-3	Имеет практический опыт: владения профессиональной терминологией в области информационной безопасности, с учетом ее основных требований.	+	+	+		+
ОПК-4	Знает: структуру документов и нормативные требования к их составлению в области защита информации и кибербезопасности.		+		+	+
ОПК-4	Умеет: разрабатывать технические задания на создание подсистем защита информации и кибербезопасности.		+		+	+
ОПК-4	Имеет практический опыт: работы с документами в области защита информации и кибербезопасности.		+			+
ПК-3	Знает: основы организационной защита информации при работе с компонентами аппаратно-программных комплексов и программным обеспечением.	+		+	+	+
ПК-3	Умеет: анализировать требования к компонентам аппаратно-программных комплексов и программному обеспечению и выполнять защиту информации на физическом и программном уровнях.	+		+	+	+
ПК-3	Имеет практический опыт: методами организации защиты информации на физическом и программных уровнях.	+		+	+	+

Типовые контрольные задания по каждому мероприятию находятся в приложениях.

7. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) основная литература:

Не предусмотрена

б) дополнительная литература:

1. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей [Текст]/ В.Ф. Шаньгин.- М.: ИД «ФОРУМ»: ИНФРА-М, 2011.- 416 с. - ISBN 978-5 8199-0331-5

2. Малюк, А.А. Введение в защиту информации в автоматизированных системах [Текст]: учебное пособие для вузов / А.А. Малюк, С.В. Пазизин, Н.С.Погожин. – 2-е изд. – М.: Горячая линия – Телеком, 2004. – 147с.: ил.- ISBN 5-93517-062-0.

3. Хорев, П.Б. Методы и средства защиты информации в компьютерных системах [Текст]: учебное пособие для студентов вузов / П.Б. Хорев.- М.: Академия, 2006.- 256с.- ISBN 5-7695-1839-1.

в) отечественные и зарубежные журналы по дисциплине, имеющиеся в библиотеке:

1. Программирование

г) методические указания для студентов по освоению дисциплины:

1. Организационная защита информации: методические указания по выполнению самостоятельной работы для обучающихся по направлению 09.03.01 Информатика и вычислительная техника/ Л.Н.Буйлушкина Нижневартовск, 2022. – 9 с.

из них: учебно-методическое обеспечение самостоятельной работы студента:

1. Организационная защита информации: методические указания по выполнению самостоятельной работы для обучающихся по направлению 09.03.01 Информатика и вычислительная техника/ Л.Н.Буйлушкина Нижневартовск, 2022. – 9 с.

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Дополнительная литература	Электронно-библиотечная система Znanium.com	Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2024. — 336 с. — ISBN 978-5-369-01761-6. https://znanium.ru/catalog/product/208264
2	Дополнительная литература	Электронно-библиотечная система Znanium.com	Глинская, Е. В. Информационная безопасность конструкций ЭВМ и систем : учебное пособие / Е.В. Глинская, Н.В. Чичварин. — Москва : ИНФРА-М, 2021. — 118 с. — ISBN 978-5-16-010961-9. https://znanium.ru/catalog/product/1178152
3	Основная литература	ЭБС издательства Лань	Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. https://e.lanbook.com/book/156401
4	Основная литература	ЭБС издательства Лань	Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии : учебник / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2022. — 344 с. — ISBN 978-5-8114-3940-9. https://e.lanbook.com/book/207095

Перечень используемого программного обеспечения:

1. Microsoft-Office(бессрочно)
2. ФГАОУ ВО "ЮУрГУ (НИУ)"-Портал "Электронный ЮУрГУ" (https://edu.susu.ru)(бессрочно)
3. -Borland Developer Studio(бессрочно)

Перечень используемых профессиональных баз данных и информационных справочных систем:

1. ООО "Консультант Плюс Югра"-Консультант Плюс (Нижневартовск)(31.12.2026)

8. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Лекции		Занятия студентов проходят в лекционных и компьютерных аудиториях филиала. Основная и дополнительная литература, словари находятся в фондах библиотеки филиала, где также организован доступ к материалам электронных библиотечных систем
Практические занятия и семинары		Предустановленное программное обеспечение: ОС Windows 7 Professional; Денвер; MS SQL Server 2008R2; Oracle VM VirtualBox; Microsoft Office 2010; Информационно-правовая база «Консультант – Плюс»; DOSBox