МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Смоленский казачий институт промышленных технологий и бизнеса (филиал) федерального государственного бюджетного образовательного учреждения «Московский государственный университет технологий и управления имени К.Г. Разумовского (Первый казачий университет)»

Смоленский казачий институт промышленных технологий и бизнеса (филиал)

УТВЕРЖДАЮ
Директор СКИПТБ (филиал) ФГБОУ ВО
«МГУТУ им. К.Г. Разумовского (ПКУ)
_____ Н.С. Коржикова
«21» апреля 2026 г.

Рабочая программа дисциплины (модуля)

Б1.О.04.11 ОБЩЕПРОФЕССИОНАЛЬНЫЙ МОДУЛЬ Информационная безопасность

Кафедра:	Системной автоматизации и информационных технологий
Направление подготовки:	09.03.01 Информатика и вычислительная техника
Направленность (профиль):	Проектирование и разработка программного обеспечения
Квалификация выпускника:	Бакалавр
Форма обучения:	очная
Год набора:	2026
Общая трудоемкость:	216 часов/6 з.е.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 00F5 665F CCDB 5046 05DD 6E08 EBCB D00A DC
Действителен: с 21 октября 2025 г. по 14 января 2027 г.
Владелец: Коржикова Надежда Сергеевна
Должность: Директор

Вязьма, 2026 г.

Программу составил(и):
ст. преподаватель Иванов Андрей Александрович

Рабочая программа дисциплины (модуля)
"Информационная безопасность"
разработана на основании учебного плана, утвержденного ученым советом 26 марта 2026 г. протокол № 9 в соответствии с ФГОС ВО Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 09.03.01 Информатика и вычислительная техника (приказ Минобрнауки России от 19.09.2017 г. № 929),

Руководитель ОПОП
канд. пед. наук, доцент Кузьмин К.А._____

Рабочая программа обсуждена на заседании обеспечивающей кафедры
Системной автоматизации и информационных технологий
Протокол от 10 апреля 2026 г. № 9
Зав. кафедрой Кузьмин Константин Анатольевич_____

СОДЕРЖАНИЕ

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ И ОБЪЕМ С РАСПРЕДЕЛЕНИЕМ ПО СЕМЕСТРАМ

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫЕ С РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

6. ОЦЕНОЧНЫЕ И МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

9. ОРГАНИЗАЦИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Цели:

Цель учебной дисциплины заключается в получении обучающимися теоретических знаний и практических навыков в области информационной безопасности

1.2. Задачи:

1. изложение теоретических основ информационной безопасности;
2. изучение нормативно-правовой базы в области информационной безопасности в РФ, включая нормативно-правовое регулирование защиты персональных данных;
3. ознакомление с современными криптографическими алгоритмами и возможностями технической защиты информации;
4. приобретение навыков работы по обеспечению пользовательской безопасности и безопасности персональных данных.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ И ОБЪЕМ С РАСПРЕДЕЛЕНИЕМ ПО СЕМЕСТРАМ

Цикл (раздел) ОП: "Информационная безопасность"

Дисциплина относится к обязательной части ОПОП и обязательна для освоения.

Распределение часов дисциплины

Семестр (<Курс>.<Семестр на курсе>)	**5 (3.1)**		**6 (3.2)**		Итого	
Недель	17 1/6		17 1/6			
Вид занятий	УП	РП	УП	РП	УП	РП
Лекции	16	16	16	16	32	32
Лабораторные			16	16	16	16
Практические	16	16	16	16	32	32
В том числе в форме практ.подготовки			4	4	4	4
Итого ауд.	32	32	48	48	80	80
Контактная работа	32	32	48	48	80	80
Сам. работа	40	40	69	69	109	109
Часы на контроль			27	27	27	27
Итого	72	72	144	144	216	216

Вид промежуточной аттестации:

Зачёт 5 семестр

Экзамен 6 семестр

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫЕ С РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины (модуля) направлен на формирование следующих компетенций и индикаторов их

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;

ОПК-3.1: Знает принципы информационной и библиографической культуры, методы и средства решения стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ОПК-3.2: Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ОПК-3.3: Владеет методами поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций, на основе информационной и библиографической культуры с учетом соблюдения авторского права и требований информационной безопасности

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	**Наименования разделов, тем, их краткое содержание и результаты освоения /вид занятия/**	**Семестр**	**Часы**	**Интеракт.**	**Прак. подг.**	**Индикаторы достижения компетенции**	**Виды контроля**

	Раздел 1.Раздел 1. История и современные методы криптографической защиты информации						
1.1	**История и современные методы криптографической защиты информации** **Краткое описание: эволюция криптографии (от шифра Цезаря до асимметричных алгоритмов), фундаментальные задачи обеспечения конфиденциальности, целостности и аутентификации данных, а также устройство и применение криптографических хеш-функций (MD5, SHA-256) с практической реализацией в C#.** **Знать: различия между симметричной и асимметричной криптографией, принципы работы хеш-функций (особенности MD5 и SHA-256, их сильные стороны и уязвимости), а также понимать, как обеспечиваются конфиденциальность, целостность и аутентификация информации с помощью шифрования, хеширования и электронной подписи. /Лек/**	5	16	0	0	ОПК-3.1	Устный опрос
1.2	**Практическая работа 1.1. Сравнение данных с помощью хэш-функции** **Краткое описание: криптографические хэш-функции, их основные свойства (детерминированность, односторонность, устойчивость к коллизиям, чувствительность к изменениям), сравниваются алгоритмы MD5 и SHA-256 (длина хеша, стойкость, рекомендации). Приводится практическая реализация вычисления хешей на C# с использованием пространства имён System.Security.Cryptography, демонстрируется влияние кодировки (UTF-8) на результат и невозможность восстановления исходных данных по хешу.** **Уметь: вычислять MD5 и SHA-256 хеши для строковых данных в C#, правильно преобразовывать входные данные в массив байтов с указанием кодировки UTF-8, а также сравнивать полученные хеши для проверки целостности и выявления изменений в исходном сообщении.** **Владеть: навыками реализации хэш-функций в среде .NET с использованием классов MD5 и SHA256, метода ComputeHash(), а также преобразования байтового массива в шестнадцатеричную строку для последующего визуального сравнения хеш-кодов. /Пр/**	5	8	0	0	ОПК-3.2,ОПК-3.3	Отчет о выполнении практической работы
1.3	**Практическая работа 1.2.**	5	8	0	0	ОПК-	Отчет о выполнении

	Стеганографические методы защиты информации **Краткое описание: принципы стеганографии как скрытой передачи информации, отличие от криптографии, классификация стеганографических методов. Основное внимание уделено методу замены младшего значащего бита (LSB) для внедрения текстовых сообщений в изображения формата BMP. Приводятся математические основы метода, реализация на C# с использованием System.Drawing, а также расширенный вариант с предварительным шифрованием AES. Демонстрируется оценка визуальных и статистических изменений, расчёт ёмкости контейнера.** **Уметь: реализовывать на C# внедрение и извлечение текстового сообщения в растровое изображение (BMP) методом LSB, правильно преобразовывать сообщение в битовую последовательность, изменять младшие биты цветовых каналов пикселей, а также рассчитывать максимальный объём скрываемых данных для заданного изображения.** **Владеть: навыками работы с классами Bitmap, Color, ImageFormat в пространстве имён System.Drawing, методами побитовых операций (маскирование, сдвиги), а также приёмами повышения скрытности (предварительное шифрование сообщения, использование префикса длины) и базовыми методами стегоанализа (сравнение гистограмм, процент изменённых пикселей). /Пр/**					3.2,ОПК-3.3	практической работы
1.4	**История и современные методы криптографической защиты информации** **Краткое описание: современные программно-аппаратные средства защиты (антивирусы, фаерволы, VPN, SIEM) и вызовы, связанные с развитием квантовых вычислений.** **Знать: классификацию и назначение основных программно-аппаратных средств защиты информации (антивирусы, межсетевые экраны, системы обнаружения и предотвращения вторжений IDS/IPS, VPN, SIEM, системы резервного копирования), а также понимать суть угрозы квантовых компьютеров для асимметричных криптоалгоритмов (RSA, ECC) и направления развития постквантовой криптографии.** **Уметь: различать функции**	5	40	0	0	ОПК-3.1,ОПК-3.2,ОПК-3.3	Вопросы для самоподготовки

	различных средств защиты (например, фаервол – фильтрация трафика, SIEM – агрегация и анализ событий, VPN – шифрованный туннель), объяснять, почему квантовый алгоритм Шора подрывает стойкость факторизации и дискретного логарифмирования, и приводить примеры многофакторной аутентификации как альтернативы паролям. Владеть: понятийным аппаратом в области современных систем информационной безопасности, навыками выбора адекватных комбинаций средств защиты для создания многоуровневой обороны, а также способностью анализировать перспективы развития криптографии в условиях роста вычислительных мощностей и появления квантовых технологий. /Ср/						
1.5	**Зачёт ОПК-3.1: Знает принципы информационной и библиографической культуры, методы и средства решения стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности ОПК-3.2: Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности ОПК-3.3: Владеет методами поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций, на основе информационной и библиографической культуры с учетом соблюдения авторского права и требований информационной безопасности /Зачёт/**	5	0	0	0	ОПК-3.1,ОПК-3.2,ОПК-3.3	Вопросы к зачёту, итоговое тестирование
	Раздел 2.Раздел 2. Нормативно-правовое регулирование информационной безопасности в РФ.						
2.1	**Практическая работа 2.1. Организация защиты персональных данных Краткое описание: Изучение требований российского законодательства (ФЗ-152 «О персональных данных», ФЗ-98 «О коммерческой тайне») и национальных криптографических стандартов (ГОСТ 34.11-2018**	6	8	0	0	ОПК-3.2,ОПК-3.3	Отчет о выполнении практической работы

	«Функция хэширования», ГОСТ 34.12-2018 «Блочные шифры»). Рассматриваются этапы организации защиты персональных данных (ПДн): определение целей обработки, классификация ИСПДн, разработка документов, реализация технических мер (шифрование, хэширование, разграничение доступа), обучение сотрудников и оценка соответствия. На практическом примере оператора онлайн-такси анализируются субъекты и категории ПДн, правовые основания обработки, применение криптостандартов для защиты конфиденциальности и целостности, а также составляется проект уведомления об обработке ПДн для пользователей. Уметь: на основе ФЗ-152 определять субъекта, оператора и обработчика ПДн в конкретной ситуации, классифицировать категории ПДн (включая биометрические и специальные), обосновывать правовые основания обработки, а также подбирать адекватные криптографические средства (хэширование – для целостности и аутентификации, шифрование – для конфиденциальности) для защиты ПДн при передаче и хранении. Владеть: навыками разработки фрагментов организационно-распорядительной документации (уведомление об обработке ПДн, политика обработки), умением применять требования статей 6, 18.1, 19 ФЗ-152 для построения системы защиты ПДн, а также способностью соотносить технические меры (шифрование по ГОСТ 34.12, хэширование по ГОСТ 34.11) с конкретными задачами обеспечения безопасности персональных данных. /Пр/						
2.2	**Организация защиты персональных данных Краткое описание: Комплексное изучение базовых нормативных документов, регулирующих защиту информации в Российской Федерации. ФЗ-152 устанавливает правовые основы обработки и защиты персональных данных, права субъектов и обязанности операторов. ФЗ-98 определяет режим коммерческой тайны и меры по её охране. ГОСТ Р 34.11–2012 (алгоритм «Стрибог») задает криптографическую хэш-функцию для обеспечения целостности данных и проверки подлинности. ГОСТ Р 34.12–2015 описывает блочные шифры («Кузнечик» и**	6	34	0	0	ОПК-3.1,ОПК-3.2,ОПК-3.3	Вопросы для самоподготовки

	«Магма») для шифрования конфиденциальной информации. Знать: ключевые положения ФЗ-152 (понятия ПДн, оператора, обработки, согласия субъекта, требования к безопасности), основные принципы ФЗ-98 (понятие коммерческой тайны, режим конфиденциальности, обязанности обладателя информации), а также назначение и область применения национальных криптостандартов: хэш-функция по ГОСТ Р 34.11 – для вычисления дайджеста и контроля целостности; блочные шифры по ГОСТ Р 34.12 – для шифрования данных с длиной блока 128 бит и ключами 128/256 бит. Уметь: различать категории ПДн по ФЗ-152 (общедоступные, специальные, биометрические, иные), определять основания обработки ПДн без согласия субъекта, применять положения ФЗ -98 для отнесения информации к коммерческой тайне, а также объяснять, в каких ситуациях используется хэширование (проверка целостности файлов, хэширование паролей, электронная подпись), а в каких – блочное шифрование (защита конфиденциальных данных при хранении и передаче). Владеть: понятийным аппаратом российского законодательства в области персональных данных и коммерческой тайны, навыками анализа операторской деятельности на соответствие ФЗ-152, умением выбирать криптографические механизмы (хэширование или шифрование) согласно поставленным задачам защиты, а также способностью ориентироваться в требованиях национальных стандартов для построения систем криптографической защиты информации. /Ср/						
	Раздел 3.Раздел 3. Информационная безопасность пользователя						
3.1	**Информационная безопасность пользователя Краткое описание: основные угрозы информационной безопасности в современном цифровом мире (вредоносное ПО, социальная инженерия, утечки данных, риски мобильных устройств и IoT). Излагаются криптографические основы защиты данных: симметричное (AES) и асимметричное шифрование, режимы работы, атаки по побочным каналам.**	6	16	0	0	ОПК-3.1	Устный опрос

	Приводится практическая реализация шифрования на C# с использованием System.Security.Cryptography. Освещаются вопросы защиты баз данных (SQL Server: аутентификация, шифрование, Row-Level Security, аудит), организационно-правовые меры (ФЗ-152, ФЗ-98, ISO 27001), управление инцидентами. Анализируются технические средства защиты пользовательских устройств (антивирусы, EDR, VPN, MDM), безопасность веб-приложений (OWASP Top 10, MFA, CSP). Обсуждаются социальные аспекты (культура безопасности, психология восприятия рисков) и будущие вызовы (квантовые вычисления, постквантовая криптография, искусственный интеллект, Zero Trust). Знать: основные виды угроз информационной безопасности пользователя, принципы работы симметричных (AES) и асимметричных алгоритмов, организационные и технические меры защиты данных, а также ключевые концепции современной безопасности: Zero Trust, постквантовую криптографию и управление инцидентами. /Лек/						
3.2	**Практическая работа 3.1. Блокирование рекламы и нежелательных объектов на веб-страницах Краткое описание: Приобретение практических навыков блокировки рекламы, трекеров и вредоносных доменов с использованием различных технологий: браузерного расширения uBlock Origin (фильтры, ручное добавление правил), системного файла hosts (перенаправление на локальный адрес) и сетевых DNS-фильтров (на примере Pi-hole). Изучаются принципы работы блокировщиков на разных уровнях (браузер, ОС, сеть), форматы правил фильтрации, анализ сетевых запросов через инструменты разработчика, а также влияние блокировки на скорость загрузки и совместимость с легитимными сервисами. Уметь: устанавливать и настраивать браузерное расширение uBlock Origin, включать необходимые списки фильтров (EasyList, RU AdList), анализировать сетевые запросы на вкладке «Сеть» инструментов разработчика, выявлять подозрительные домены (содержащие ad, track, pixel),**	6	8	0	4	ОПК-3.2,ОПК-3.3	Отчет о выполнении практической работы

	создавать временные правила блокировки в формате ||domain.com^ или ||domain.com/path^, редактировать системный файл hosts с правами администратора, добавлять строки с перенаправлением рекламных доменов на 127.0.0.1 или 0.0.0.0, очищать DNS-кэш командой ipconfig /flushdns, а также объяснять настройки клиентского устройства для использования сетевого DNS-фильтра (Pi-hole). **Владеть: навыками практической настройки средств блокировки нежелательного контента на пользовательском устройстве, приёмами ручного добавления правил фильтрации при обнаружении не заблокированной автоматически рекламы, методами проверки эффективности блокировки (сравнение отображения страницы до и после, анализ счётчиков в расширении), а также умением оценивать достоинства и недостатки каждого подхода (браузерный блокировщик – гибкость, но потребление ресурсов; hosts – системный уровень, но требует ручного обновления; DNS-фильтр – защита всех устройств в сети, но не блокирует контент на уровне кода страницы). /Пр/**						
3.3	**Лабораторная работа 3.2. Исследование методов защиты паролей пользователя** **Краткое описание: В работе изучаются современные методы криптографической защиты паролей: хэширование (MD5, SHA-1, SHA-256), использование уникальной «соли» (salt) для предотвращения атак с радужными таблицами, а также алгоритмы ключевого растяжения (PBKDF2, bcrypt, Argon2). Практически сравниваются уязвимости устаревших алгоритмов (MD5, SHA-1) с помощью онлайн-сервисов взлома хэшей, демонстрируется влияние соли на уникальность хэша для одинаковых паролей, а также оценивается замедление вычислений при увеличении числа итераций в PBKDF2.** **Рассматриваются основные угрозы (атака по словарю, brute-force, радужные таблицы) и современные рекомендации (хранение паролей в виде «хэш + соль» с ключевым растяжением).** **Уметь: различать сильные и слабые хэш-алгоритмы применительно к защите паролей, генерировать случайную соль и вычислять хэш пароля с солью,**	6	8	0	0	ОПК-3.2,ОПК-3.3	Отчет о выполнении лабораторной работы

	использовать онлайн-сервисы (CrackStation, md5decrypt.net) или утилиты (hashcat) для демонстрации уязвимости MD5 и SHA-1, а также оценивать время вычисления обычного хэша (SHA-256) и адаптивной функции (PBKDF2) с разными параметрами итераций. Владеть: навыками практической проверки стойкости парольных хэшей, умением объяснить, почему соль делает неэффективными радужные таблицы и предотвращает обнаружение одинаковых паролей у разных пользователей, а также пониманием влияния параметра сложности (числа итераций) на баланс между безопасностью и удобством использования (время аутентификации). Студент должен быть способен обоснованно выбирать современный метод хранения паролей (Argon2, bcrypt или PBKDF2 с высокой итерацией) в зависимости от требований системы. /Лаб/						
3.4	**Лабораторная работа 3.3. Антивирусное программное обеспечение Краткое описание: В работе изучаются классификация вредоносного ПО (вирусы, черви, трояны, шпионское ПО, руткиты, вымогатели, боты) и основные методы обнаружения угроз: сигнатурный анализ (по базам сигнатур), эвристический (поведенческий) анализ, проактивная защита (HIPS), облачные технологии и песочница. Практически выполняются: установка и анализ интерфейса двух антивирусных продуктов (коммерческого и бесплатного), проверка эффективности сигнатурного и эвристического методов с использованием тестового файла EICAR (в том числе модифицированного), исследование возможностей проактивной защиты при попытках подозрительных действий (создание файлов в системной директории, запуск процессов), а также сравнительный анализ продуктов по критериям (наличие компонентов, реакция на тесты, удобство). Уметь: различать основные типы вредоносного ПО и методы их обнаружения, устанавливать и настраивать антивирусное ПО (включая включение модулей проактивной защиты), создавать тестовый файл EICAR, проводить выборочное сканирование,**	6	8	0	0	ОПК-3.2,ОПК-3.3	Отчет о выполнении лабораторной работы

	анализировать реакцию антивируса на стандартную и модифицированную сигнатуру, выполнять подозрительные действия в изолированной среде (виртуальной машине) для проверки поведенческих анализаторов, а также заполнять сравнительную таблицу по заданным критериям. Владеть: навыками практической работы с антивирусными продуктами (просмотр компонентов, журналов, карантина, настройка сканирования), умением интерпретировать результаты сигнатурного и эвристического анализов, навыками оценки эффективности проактивной защиты при блокировке подозрительных действий (запись в системные директории, запуск утилит из неподписанных приложений), а также способностью обосновывать выбор антивирусного решения для различных сценариев (домашний компьютер, малый офис) с учётом баланса между защитой и нагрузкой на систему. /Лаб/						
3.5	**Информационная безопасность пользователя Краткое описание: Изучение синхронных (симметричных) методов шифрования на примере алгоритма AES (Advanced Encryption Standard) – его история, структура (сеть замещения–перестановки), размеры блока и ключа (128/192/256 бит), количество раундов, основные этапы преобразований (SubBytes, ShiftRows, MixColumns, AddRoundKey). Преимущества и недостатки симметричного шифрования, необходимость защиты файлов от утечек и кражи. Приводится практическая реализация шифрования и расшифрования файлов на C# с использованием класса Aes, потоков CryptoStream, FileStream, а также управление ключами и вектором инициализации (IV). Вопросы создания базы данных SQL Server в среде Visual Studio: добавление нового элемента «База данных, основанная на службах», создание таблиц с помощью оператора CREATE TABLE, определение первичных и внешних ключей (PRIMARY KEY, FOREIGN KEY), установление связей между таблицами (один к одному, один ко многим, многие ко многим).**	6	35	0	0	ОПК-3.1,ОПК-3.2,ОПК-3.3	Вопросы для самоподготовки

	Знать: принципы симметричного шифрования, структуру и параметры алгоритма AES (длина блока 128 бит, ключи 128/192/256 бит, количество раундов 10/12/14), основные этапы одного раунда; понимать необходимость шифрования файлов для обеспечения конфиденциальности и соответствия нормативным требованиям; знать основы реляционных баз данных: создание таблиц, типы данных, ограничения (NOT NULL, PRIMARY KEY, FOREIGN KEY), типы связей. Уметь: реализовывать на C# шифрование и расшифрование файлов с использованием AES-256: создавать экземпляр Aes, генерировать или устанавливать ключ и вектор инициализации, применять CryptoStream для чтения/записи зашифрованных данных, корректно освобождать ресурсы с помощью using. Также уметь создавать базу данных SQL Server в Visual Studio, добавлять таблицы, определять столбцы с соответствующими типами данных и устанавливать связи между таблицами через внешние ключи. Владеть: навыками работы с пространством имён System.Security.Cryptography в .NET, навыками потокового шифрования (FileStream, CryptoStream, MemoryStream), преобразования зашифрованных байтов в строку Base64. Владеть навыками проектирования реляционной схемы базы данных, написания SQL-запросов CREATE TABLE с ограничениями, а также подключения созданной базы данных к приложению через источники данных. /Ср/						
3.6	**Экзамен** **ОПК-3.1: Знает принципы информационной и библиографической культуры, методы и средства решения стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности** **ОПК-3.2: Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности** **ОПК-3.3: Владеет методами поиска и анализа информации для**	6	27	0	0	ОПК-3.1,ОПК-3.2,ОПК-3.3	Вопросы к экзамену, итоговое тестирование

	подготовки документов, обзоров, рефератов, докладов, публикаций, на основе информационной и библиографической культуры с учетом соблюдения авторского права и требований информационной безопасности /Экзамен/						

Перечень применяемых активных и интерактивных образовательных технологий:

Информационные технологии

Личностно ориентированная технология, способ организации самостоятельной деятельности учащихся, направленный на решение задачи учебного проекта

Проектная технология

Стандартизированный метод оценки знаний, умений, навыков учащихся, который помогает выявить и сформировать индивидуальный темп обучения, пробелы в текущей итоговой подготовке

Технология модульного обучения

Технология модульного обучения основана на идее личностно-ориентированного подхода. Основной технологии модульного обучения является самостоятельное освоение учебных дисциплин, которые для удобства поделены на модули. Цель технологии модульного обучения – создать условия выбора для полного овладения содержанием образовательных программ в разной последовательности, разном объеме и темпе через отдельные и независимые учебные модули с учетом индивидуальных интересов и возможностей субъектов образовательного процесса

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Самостоятельная (внеаудиторная) работа обучающегося (далее - СРС) – это планируемая учебная, практическая, учебно-исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное время (свободное от аудиторных учебных занятий) по заданию и при методическом руководстве научно-педагогического работника (далее – преподаватель) и (или) лиц, привлекаемых к реализации основных профессиональных образовательных программ на иных условиях, но без их непосредственного участия.

СРС по заданию и при методическом руководстве преподавателя и (или) лиц, привлекаемых к реализации основных профессиональных образовательных программ на иных условиях, реализуется во время групповых консультаций и (или) индивидуальной работы обучающихся с преподавателями Университета и (или) лиц, привлекаемых к реализации образовательных программ на иных условиях (в том числе индивидуальных консультаций), а также во время текущего контроля выполнения заданий, отнесенных к самостоятельной работе обучающихся.

Целью СРС является овладение формирование компетенций через овладение знаниями, умениями и навыками профессиональной деятельности по направлению подготовки (специальности). Самостоятельная работа является обязательной для каждого обучающегося.

Формы самостоятельной работы обучающихся определяются преподавателями кафедр Университета при разработке рабочих программ дисциплин (модулей), рабочих программ практик, программ государственной итоговой (итоговой) аттестации, методических указаний по выполнению практических, лабораторных работ, написанию курсовых работ/проектов и ВКР в соответствии с их содержанием.

В Университете оборудованы специальные помещения для самостоятельной работы обучающихся. Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к информационно -телекоммуникационной сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Университета.

6. ОЦЕНОЧНЫЕ И МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

6.1. Перечень компетенций с указанием уровней их сформированности

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;

Недостаточный уровень:

Знает принципы информационной культуры

Умеет решать стандартные задачи профессиональной деятельности

Владеет методами поиска и анализа информации для подготовки документов

Пороговый уровень:

Знает принципы информационной и библиографической культуры

Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры

Владеет методами поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций

Продвинутый уровень:

Знает принципы информационной и библиографической культуры, методы и средства решения стандартных задач профессиональной деятельности

Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий

Владеет методами поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций, на основе информационной и библиографической культуры

Высокий уровень:

Знает принципы информационной и библиографической культуры, методы и средства решения стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Владеет методами поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций, на основе информационной и библиографической культуры с учетом соблюдения авторского права и требований информационной безопасности

6.2. Описание критериев оценивания успеваемости

НЕДОСТАТОЧНЫЙ УРОВЕНЬ	ПОРОГОВЫЙ УРОВЕНЬ	ПРОДВИНУТЫЙ УРОВЕНЬ	ВЫСОКИЙ УРОВЕНЬ
Обучающийся демонстрирует: - существенные пробелы в знаниях учебного материала; - принципиальные ошибки при ответе на основные вопросы билета, отсутствует знание и понимание основных понятий и категорий; - непонимание сущности дополнительных вопросов в рамках заданий билета; - отсутствие умения выполнять практические задания, предусмотренные программой дисциплины (модуля); - отсутствие готовности (способности) к дискуссии и низкая степень контактности.	Обучающийся демонстрирует: - знания теоретического материала; - неполные ответы на основные вопросы, ошибки в ответе, недостаточное понимание сущности излагаемых вопросов; - неуверенные и неточные ответы на дополнительные вопросы; - недостаточное владение литературой, рекомендованной программой дисциплины (модуля); - умение без грубых ошибок решать практические задания, которые следует выполнить.	Обучающийся демонстрирует: - знание и понимание основных вопросов контролируемого объема программного материала; - твердые знания теоретического материала; - способность устанавливать и объяснять связь практики и теории, выявлять противоречия, проблемы и тенденции развития; - правильные и конкретные, без грубых ошибок ответы на поставленные вопросы; - умение решать практические задания, которые следует выполнить; - владение основной литературой, рекомендованной программой дисциплины (модуля); - наличие собственной обоснованной позиции по обсуждаемым вопросам; - незначительные оговорки и неточности в раскрытии отдельных положений вопросов билета, присутствует неуверенность в ответах на дополнительные вопросы.	Обучающийся демонстрирует: - глубокие, всесторонние и аргументированные знания программного материала; - полное понимание сущности и взаимосвязи рассматриваемых процессов и явлений, точное знание основных понятий в рамках обсуждаемых заданий; - способность устанавливать и объяснять связь практики и теории; - логически последовательные, содержательные, конкретные и исчерпывающие ответы на все задания билета, а также дополнительные вопросы экзаменатора; - умение решать практические задания; - свободное использование в ответах на вопросы материалов рекомендованной основной и дополнительной литературы.
Оценка «незачет», «неудовлетворительно»	**Оценка «зачтено/удовлетворительно», «удовлетворительно»**	**Оценка «зачтено/хорошо», «хорошо»**	**Оценка «зачтено/отлично», «отлично»**

6.3. Оценочные средства текущего контроля

Вопросы для устного опроса.

Тема 1. История и современные методы криптографической защиты информации

1. Дайте определение криптографии. Какие три фундаментальные задачи она решает (конфиденциальность, целостность, аутентификация)? Поясните каждую.
2. В чём отличие шифрования от хеширования? Приведите примеры алгоритмов для каждого преобразования.
3. Опишите принцип работы симметричной криптографии. В чём заключается проблема распределения ключей?
4. Объясните концепцию асимметричной криптографии (с открытым ключом). Как она решает проблему распределения ключей?
5. Назовите известные симметричные алгоритмы (DES, Triple DES, AES). Какова длина ключа в AES и количество

7. Дайте определение криптографической хеш-функции. Перечислите три основных свойства стойкой хеш-функции.
8. Опишите алгоритм MD5: какова длина хеша, история создания, почему признан небезопасным? Какие атаки на него существуют?
9. Что такое коллизия хеш-функции? Почему коллизии в MD5 делают его непригодным для цифровых подписей?
10. Расскажите о семействе SHA-2 и алгоритме SHA-256. Какова длина хеша, на какой структуре основан, где применяется (блокчейн Bitcoin, TLS/SSL)?
11. Какие программно-аппаратные средства защиты информации вы знаете? Опишите назначение антивируса, фаервола, VPN, SIEM.
12. Чем отличаются системы обнаружения вторжений (IDS) от систем предотвращения вторжений (IPS)?
13. Для чего используется система резервного копирования (бэкап) в контексте информационной безопасности?
14. Какую угрозу несут квантовые компьютеры для современной криптографии? Что такое алгоритм Шора и против каких алгоритмов он эффективен?
15. Что такое постквантовая криптография? Какие алгоритмы считаются перспективными для защиты от квантовых атак?

Тема 3. Информационная безопасность пользователя
1. Дайте определение информационной безопасности пользователя. Почему пользователь часто является самым слабым звеном в системе безопасности?
2. Перечислите основные виды технических угроз (вредоносное ПО, шифровальщики, бот-сети, APT-атаки). Что такое целевая атака?
3. Объясните метод социальной инженерии. Приведите пример фишинга и spear-phishing.
4. Какие угрозы связаны с использованием мобильных устройств и интернета вещей (IoT)? Почему IoT-устройства особенно уязвимы?
5. В чём разница между симметричным и асимметричным шифрованием? Приведите примеры алгоритмов.
6. Опишите режимы работы блочных шифров: ECB, CBC, GCM. Какой из них обеспечивает одновременно конфиденциальность и целостность?
7. Что такое атаки по побочным каналам (side-channel attacks)? Как можно противодействовать таким атакам в программной реализации?
8. Как реализовать шифрование файлов на C# с использованием AES? Какие классы и пространства имён используются (System.Security.Cryptography, CryptoStream, Aes.Create())?
9. Какие механизмы безопасности предоставляют современные СУБД (SQL Server)? Объясните прозрачное шифрование данных (TDE) и Row-Level Security.
10. Что такое первичный и внешний ключ в реляционной базе данных? Приведите SQL-синтаксис для создания таблицы с внешним ключом.
11. Назовите основные организационные меры информационной безопасности (политика безопасности, управление доступом, обучение сотрудников, разделение обязанностей).
12. Что такое управление инцидентами (Incident Response)? Перечислите основные фазы цикла реагирования на инциденты.
13. Какие правовые документы регулируют защиту персональных данных в РФ? Кратко охарактеризуйте ФЗ-152 и ФЗ-98.
14. Опишите, как защитить пользовательское устройство (компьютер/ноутбук/смартфон). Какие меры являются ключевыми (обновления, антивирус, шифрование диска, VPN)?
15. Что такое Zero Trust (нулевое доверие) и чем эта модель отличается от традиционной периметральной защиты?

Вопросы для самоподготовки.
Тема 1.
1. Перечислите основные этапы эволюции криптографии от древности до наших дней. Какие исторические шифры (шифр Цезаря, шифр Виженера) и в чём их недостатки?
2. Сформулируйте три фундаментальные задачи криптографии: конфиденциальность, целостность и аутентификация. Приведите примеры криптографических механизмов для каждой задачи.
3. В чём различие между симметричной и асимметричной криптографией? Объясните проблему распределения ключей в симметричных системах и как её решает асимметричная криптография.
4. Что такое электронная цифровая подпись (ЭЦП)? Какие криптографические примитивы используются для её построения?
5. Опишите структуру и параметры алгоритма AES: размер блока, длины ключей, количество раундов для каждого размера ключа. Какие основные операции выполняются в каждом раунде?
6. На чём основана криптостойкость алгоритма RSA? Какую роль играет факторизация больших чисел? Каковы рекомендуемые длины ключей на сегодняшний день?
7. Дайте определение криптографической хеш-функции. Объясните свойства: устойчивость к прообразу, устойчивость ко второму прообразу, устойчивость к коллизиям.
8. Изучите самостоятельно алгоритм MD5 (длина хеша, история, раунды). Почему он считается небезопасным? Какие атаки (например, метод дней рождения, радужные таблицы) позволяют находить коллизии?
9. Что такое семейство SHA-2? Каковы длины хешей у SHA-256, SHA-384, SHA-512? Где применяется SHA-256 (Bitcoin, TLS/SSL, цифровые подписи)?
10. Изучите структуру Меркле-Дамгарда, лежащую в основе SHA-256. Какие константы инициализации используются и почему?
11. Перечислите и дайте краткую характеристику основным программно-аппаратным средствам защиты информации: антивирус, межсетевой экран (фаервол), IDS/IPS, VPN, SIEM, системы резервного копирования.
12. Чем отличается система обнаружения вторжений (IDS) от системы предотвращения вторжений (IPS)? Приведите примеры сигнатурных и поведенческих методов.
13. Что такое многофакторная аутентификация (MFA)? Приведите примеры факторов (знание, владение, биометрия).

7. Что такое атаки по побочным каналам (например, по времени выполнения, по энергопотреблению)? Приведите пример защитного механизма (например, выполнение операций за постоянное время).
8. Как в C# реализовать шифрование и расшифрование файлов с использованием AES? Какие классы (Aes, CryptoStream, FileStream) и методы используются? Зачем нужен блок using?
9. Что такое база данных SQL Server? Какие встроенные механизмы безопасности предоставляет СУБД (аутентификация, разграничение доступа, TDE, аудит)?
10. Что такое первичный ключ и внешний ключ? Приведите SQL-пример создания двух таблиц с отношением «один ко многим». Как обеспечивается ссылочная целостность?
11. Перечислите основные организационные меры безопасности: политика информационной безопасности, управление доступом, разделение обязанностей, планы реагирования на инциденты.
12. Опишите цикл управления инцидентами (подготовка, обнаружение, анализ, сдерживание, ликвидация, восстановление, извлечение уроков). Какая команда занимается реагированием?
13. Какие нормативно-правовые акты РФ регулируют информационную безопасность пользователей? Кратко охарактеризуйте ФЗ-152 (персональные данные) и ФЗ-149 (об информации, информационных технологиях и о защите информации).
14. Что такое Zero Trust (нулевое доверие)? В чём отличие от модели «доверять, но проверять»? Какие принципы лежат в основе Zero Trust (микросегментация, непрерывная аутентификация, наименьшие привилегии)?
15. Какие вызовы для информационной безопасности пользователя связаны с развитием интернета вещей (IoT) и искусственного интеллекта? Приведите примеры атак на IoT-устройства и использования ИИ в фишинговых кампаниях.

Задания к лабораторным и практическим работам
Практическая работа 1.1. Сравнение данных с помощью хэш-функции
Задания:
1. Разработайте консольное приложение на C#.
2. Продемонстрируйте «лавинный эффект»: покажите, что даже минимальное изменение входных данных (один символ, регистр) приводит к кардинально другому хешу.
3. Сравните длину MD5-хеша (в символах HEX) и SHA-256-хеша. Объясните разницу.
4. Оформите отчёт, включив в него листинг программы, скриншоты результатов и ответы на контрольные вопросы (из лабораторной работы №1.1).

Практическая работа 1.2. Стеганографические методы защиты информации
Задания:
1. Разработайте программу на C# (Windows Forms или консоль с использованием System.Drawing).
2. При внедрении предусмотрите:
- Преобразование сообщения в битовую последовательность.
- Запись длины сообщения (4 байта) в младшие биты первых пикселей.
- Последовательную замену младших битов каналов R, G, B пикселей битами сообщения.
3. После внедрения сравните исходное и результирующее изображения:
4. В отчёте приведите листинг программы, скриншоты исходного и стего-изображения, а также ответы на контрольные вопросы.

Практическая работа 2.1. Организация защиты персональных данных
Задания:
1. Анализ деятельности оператора. Укажите категории обрабатываемых ПДн (ФИО, телефон, геолокация, история поездок). Есть ли среди них биометрические или специальные?
2. Применение криптографических стандартов. Опишите, для каких задач в мобильном приложении и на серверах можно использовать ГОСТ 34.11-2018 (функция хэширования). Приведите пример (хэширование паролей, контроль целостности логов). Опишите, для каких задач следует использовать ГОСТ 34.12-2018 (блочное шифрование). Приведите пример (шифрование номера банковской карты, передача геолокации).
3. Разработка фрагмента документации. Составьте проект уведомления об обработке персональных данных для размещения в мобильном приложении. Уведомление должно содержать: цели обработки, перечень ПДн, способы обработки, контакты оператора.

Практическая работа 3.1. Блокирование рекламы

6.4. Оценочные средства промежуточной аттестации

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
Вопросы к зачёту
Индикатор Знать
1) Установите правильную последовательность развития методов шифрования:
а) Появление симметричных шифров
б) Изобретение шифра Цезаря
в) Создание шифрмашины Энигма
г) Разработка асимметричных шифров
2) Прочитайте текст и установите соответствие между терминами и их определениями:
А) Криптология
Б) Криптоанализ
В) Криптография
Г) Шифр
1. Наука о методах обеспечения конфиденциальности информации

2. Наука о методах вскрытия шифров
3. Общая наука о шифрах и методах их анализа
4. Система преобразования информации для обеспечения секретности
5. Метод аутентификации пользователей
3) Установите правильную последовательность появления шифров:
а) Шифр Виженера
б) Решетка Кардано
в) Шифр Цезаря
г) Одноразовый шифр-блокнот
4) Прочитайте текст и установите соответствие между методами и их характеристиками:
А) Симметричное шифрование
Б) Асимметричное шифрование
В) Цифровая подпись
Г) Атака “человек посередине”
1. Требует двух ключей для работы
2. Использует один ключ для шифрования и дешифрования
3. Обеспечивает аутентификацию и целостность
4. Представляет угрозу безопасности передачи данных
5. Метод стеганографии
5) Установите правильную последовательность этапов развития криптографии:
а) Появление механических шифрмашин
б) Развитие математических основ защиты
в) Изобретение электромагнитного телеграфа
г) Формирование научных методов защиты
6) Прочитайте текст и установите соответствие между терминами и их применением:
А) Сертификат
Б) УЦ (Удостоверяющий центр)
В) Ключ
Г) Протокол
1. Инструмент для шифрования данных
2. Документ, подтверждающий личность
3. Система правил для безопасной передачи данных
4. Организация, выдающая цифровые сертификаты
5. Метод криптоанализа
7) Установите правильную последовательность развития технологий:
а) Появление цифровых подписей
б) Развитие симметричных шифров
в) Создание шифрмашины Энигма
г) Внедрение асимметричных шифров
8) Прочитайте текст и установите соответствие между методами и их особенностями:
А) Шифр Цезаря
Б) Шифр Виженера
В) Решетка Кардано
Г) Одноразовый блокнот
1. Использует таблицу для шифрования
2. Основан на сдвиге букв
3. Применяет периодическую замену
4. Обеспечивает абсолютную секретность
5. Метод перестановки
9) Установите правильную последовательность появления технологий:
а) Появление сертификатов
б) Развитие УЦ
в) Внедрение цифровых подписей
г) Создание шифрмашин
10. Прочитайте текст и установите соответствие между терминами и их функциями:
А) Стеногрaфия
Б) Криптография
В) Цифровая подпись
Г) Сертификат
1. Метод криптоанализа
2. Метод шифрования данных
3. Инструмент аутентификации
4. Документ подтверждения личности
5. Метод скрытой передачи информации
Индикатор Уметь
11) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Какой метод шифрования обеспечивает абсолютную секретность?
а) Шифр Цезаря
б) Шифр Виженера

в) Одноразовый шифр-блокнот
г) Симметричное шифрование
12) Выберите правильные ответы и запишите аргументы, обосновывающие выбор ответа:
Какие методы шифрования используют два ключа?
а) Асимметричное шифрование
б) Симметричное шифрование
в) Шифр Энигма
г) Цифровая подпись
13) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Что такое криптоанализ?
а) Наука о методах шифрования
б) Наука о методах вскрытия шифров
в) Метод стеганографии
г) Технология создания ключей
14) Выберите правильные ответы и запишите аргументы, обосновывающие выбор ответа:
Какие характеристики присущи симметричному шифрованию?
а) Использование одного ключа
б) Высокая скорость работы
в) Сложность в управлении ключами
г) Использование двух ключей
15) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Какой метод защиты информации относится к стеганографии?
а) Шифр Цезаря
б) Решетка Кардано
в) Метод скрытой передачи данных
г) Шифр Виженера
16) Выберите правильные ответы и запишите аргументы, обосновывающие выбор ответа:
Какие преимущества имеет асимметричное шифрование?
а) Высокая скорость шифрования
б) Простота в управлении ключами
в) Возможность безопасной передачи ключей
г) Использование одного ключа
17) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Что такое атака “человек посередине”?
а) Метод шифрования данных
б) Метод криптоанализа
в) Метод перехвата и изменения данных
г) Метод аутентификации
18) Выберите правильные ответы и запишите аргументы, обосновывающие выбор ответа:
Какие функции выполняет цифровая подпись?
а) Подтверждение авторства
б) Обеспечение конфиденциальности
в) Проверка целостности данных
г) Шифрование сообщений
19) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Что такое криптографический протокол?
а) Метод шифрования данных
б) Система правил для безопасной передачи данных
в) Технология создания ключей
г) Метод криптоанализа
20) Выберите правильные ответы и запишите аргументы, обосновывающие выбор ответа:
Какие характеристики присущи шифрмашине Энигма?
а) Механическое устройство
б) Использование симметричного шифрования
в) Применение асимметричного шифрования
г) Автоматическая генерация ключей

Индикатор Владеть
21) Прочитайте текст и запишите развернутый ответ: В ходе исторического исследования были обнаружены зашифрованные послания, использовавшие шифр сцитала. Объясните принцип работы этого шифра и предположите, почему он считался надежным в свое время. Какие недостатки были у этого метода шифрования?
22) Рассчитайте количество возможных вариантов ключа для шифра Цезаря, если известно, что в алфавите используется 33 символа. Объясните, почему данный шифр считается уязвимым для современных методов криптоанализа.
23) Определите, какой метод шифрования использовался в следующем сообщении: “БМЪЛЪЖЪПЪ” (исходное сообщение “АЛФАВИТ”). Опишите алгоритм расшифровки и объясните, почему этот метод считается более надежным, чем простой шифр Цезаря.
24) Вычислите длину ключевого слова для шифра Виженера, если известно, что в зашифрованном тексте длиной 100 символов обнаружено 20 повторений определенных буквенных комбинаций через равные промежутки.
25) Прочитайте текст и запишите развернутый обоснованный ответ: В 1940-х годах немецкая армия использовала шифровальную машину “Энигма”. Объясните принцип работы этой машины и почему она считалась практически неуязвимой. Какие факторы привели к ее взлому?
26) Определите, какой метод шифрования является более надежным: симметричный или асимметричный. Приведите

Вопросы к экзамену
Индикатор Знать
1) Установите правильную последовательность этапов работы с персональными данными:
а) Классификация информации
б) Настройка политик безопасности
в) Применение технических средств защиты
г) Изучение нормативно-правовой базы
2) Прочитайте текст и установите соответствие между методами и их определениями:
А) Фишинг
Б) Претекстинг
В) Квид про Кво
Г) Тайпсвотинг
1. Метод получения информации через создание ложной ситуации
2. Метод социальной инженерии с использованием подменных веб-сайтов
3. Метод обмена информацией на информацию
4. Метод анализа клавиатурного почерка
5. Метод физического доступа к устройству
3) Установите правильную последовательность появления методов социальной инженерии:
а) Фишинг
б) Претекстинг
в) Квид про Кво
г) Обратная социальная инженерия
4) Прочитайте текст и установите соответствие между типами вредоносного ПО и их характеристиками:
А) Троянский конь
Б) Шпионское ПО
В) Вирус
Г) Червь
1. Самовоспроизводящееся ПО
2. ПО, маскирующееся под полезное
3. ПО для сбора информации
4. Самораспространяющееся ПО
5. ПО для майнинга криптовалюты
5) Установите правильную последовательность действий при настройке безопасности:
а) Создание политик паролей
б) Внедрение антивирусной защиты
в) Настройка файрвола
г) Регулярное резервное копирование
6) Прочитайте текст и установите соответствие между методами защиты и их применением:
А) Двухфакторная аутентификация
Б) Шифрование данных
В) Антивирусная защита
Г) Фильтрация контента
1. Защита от вредоносного ПО
2. Защита при передаче данных
3. Усиленная аутентификация
4. Контроль доступа к информации
5. Защита от DDoS-атак
7) Установите правильную последовательность действий при обнаружении утечки данных:
а) Уведомление регуляторов
б) Оценка масштаба утечки
в) Устранение причин
г) Информирование субъектов ПД
8) Прочитайте текст и установите соответствие между типами паролей и их характеристиками:
А) Простой пароль
Б) Композитный пароль
В) Фраза-пароль
Г) Биометрический пароль
1. Использование нескольких типов символов
2. Использование отпечатка пальца
3. Использование простой комбинации
4. Использование длинной фразы
5. Использование графического ключа
9) Установите правильную последовательность методов сбора информации:
а) Анализ открытых источников
б) Социальная инженерия
в) Физический доступ
г) Киберразведка
10) Прочитайте текст и установите соответствие между методами защиты и их функциями:

А) VPN
Б) SSL-шифрование
В) Брандмауэр
Г) Антивирус
1. Защита при передаче данных
2. Контроль сетевого трафика
3. Защита от вредоносного ПО
4. Защита веб-соединений
5. Защита от DoS-атак

Индикатор Уметь
11) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Какой метод защиты информации относится к техническим средствам?
а) Классификация данных
б) Антивирусная защита
в) Политика безопасности
г) Обучение персонала
12) Выберите правильные ответы и запишите аргументы, обосновывающие выбор ответа:
Какие характеристики относятся к стойкому паролю?
а) Использование только букв
б) Длина не менее 12 символов
в) Комбинация разных типов символов
г) Простой словарный пароль
13) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Что такое фишинг?
а) Метод физического доступа к устройству
б) Метод социальной инженерии с подменными сайтами
в) Метод криптоанализа
г) Метод стеганографии
14) Выберите правильные ответы и запишите аргументы, обосновывающие выбор ответа:
Какие методы относятся к вредоносному ПО?
а) Троянский конь
б) Антивирус
в) Вирус
г) Файрвол
15) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Что такое претекстинг?
а) Метод анализа клавиатурного почерка
б) Метод получения информации через создание ложной ситуации
в) Метод обмена информацией
г) Метод фишинга
16) Выберите правильные ответы и запишите аргументы, обосновывающие выбор ответа:
Какие способы защиты от вредоносного ПО существуют?
а) Использование антивируса
б) Регулярное резервное копирование
в) Двухфакторная аутентификация
г) Обновление ПО
17) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Что такое обратная социальная инженерия?
а) Метод сбора информации из открытых источников
б) Метод, при котором жертва сама предоставляет информацию
в) Метод фишинга
г) Метод претекстинга
18) Выберите правильные ответы и запишите аргументы, обосновывающие выбор ответа:
Какие характеристики относятся к политике безопасности?
а) Правила доступа к информации
б) Методы шифрования данных
в) Порядок реагирования на инциденты
г) Технические средства защиты
19) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Что такое “дорожное яблоко”?
а) Метод фишинга
б) Метод социальной инженерии с использованием заражённых носителей
в) Метод претекстинга
г) Метод криптоанализа
20) Выберите правильные ответы и запишите аргументы, обосновывающие выбор ответа:
Какие методы относятся к классификации информации?
а) Определение уровней конфиденциальности
б) Настройка файрвола

в) Категорирование по степени важности
г) Использование VPN

Индикатор Владеть
21) Прочитайте текст и запишите развернутый ответ: В организации произошел инцидент с утечкой персональных данных. Определите, какие нормативные акты были нарушены и какие меры наказания могут последовать согласно действующему законодательству.
22) Рассчитайте минимальный срок хранения журналов регистрации событий информационной безопасности, если организация обрабатывает специальные категории персональных данных. Обоснуйте свой ответ со ссылкой на законодательство.
23) Определите категорию конфиденциальности информации, если в документе содержатся персональные данные 1000 сотрудников, включая банковские реквизиты. Объясните выбор категории с учетом возможных рисков утечки.
24) Вычислите количество возможных комбинаций для пароля, состоящего из 8 символов (буквы, цифры, спецсимволы). Оцените его стойкость к подбору и предложите рекомендации по усилению.
25) Прочитайте текст и запишите развернутый обоснованный ответ: В компанию поступил подозрительный email от “банковского сервиса”. Опишите признаки фишингового сообщения и предложите алгоритм действий сотрудника при получении подобных писем.
26) Определите, какой метод социальной инженерии использовался, если злоумышленник представился сотрудником техподдержки и запросил пароль от учетной записи. Объясните, почему этот метод эффективен и как от него защититься.
27) Рассчитайте время, необходимое для подбора пароля, состоящего из 12 случайных символов, при скорости 1 миллиард попыток в секунду. Оцените практическую стойкость такого пароля.
28) Прочитайте текст и запишите развернутый ответ: В организации обнаружены следы вредоносного ПО. Определите основные признаки заражения и предложите порядок действий по ликвидации последствий.
29) Определите, какие технические средства защиты необходимо внедрить для предотвращения утечки персональных данных через съемные носители информации. Обоснуйте выбор каждого средства.
30) Вычислите минимальный размер выборки для аудита паролей сотрудников, если в организации работает 500 человек, с доверительной вероятностью 95%. Объясните методику расчета.

Итоговое тестирование
Зачет
1. Что является основным отличием криптографии от криптоанализа?
а) Криптография занимается созданием шифров, криптоанализ - их взломом
б) Криптография использует открытые ключи, криптоанализ - закрытые
в) Криптография работает с текстом, криптоанализ - с числами
г) Криптография использует только симметричные методы
2. Какой шифр относится к методам перестановки?
а) Шифр Цезаря
б) Шифр Виженера
в) Шифр сциталя
г) Решетка Кардано
3. Что такое одноразовый шифр-блокнот?
а) Симметричный шифр
б) Асимметричный шифр
в) Абсолютно секретный шифр
г) Метод стеганографии
4. Какие преимущества имеет асимметричное шифрование?
а) Высокая скорость работы
б) Простота реализации
в) Возможность безопасной передачи ключей
г) Низкая ресурсоемкость
5. Что такое атака “человек посередине”?
а) Перехват и изменение передаваемых данных
б) Кража ключей шифрования
в) Взлом криптосистемы
г) Социальная инженерия
6. Какой метод шифрования использует таблицу Виженера?
а) Метод замены
б) Метод перестановки
в) Метод гаммирования
г) Метод стеганографии
7. Что такое цифровая подпись?
а) Электронный аналог обычной подписи
б) Метод шифрования данных
в) Способ подтверждения авторства документа
г) Метод аутентификации пользователя
8. Какие компоненты входят в систему сертификации?
а) Центр сертификации
б) Пользовательские сертификаты
в) Криптографические ключи
г) Все вышеперечисленное
9. Что такое криптографический протокол?

б) Метод скрытой передачи информации
в) Метод криптоанализа
г) Метод аутентификации
12. Какие недостатки имеет симметричное шифрование?
а) Низкая скорость работы
б) Сложность реализации
в) Проблема безопасного обмена ключами
г) Низкая стойкость
13. Что такое сертификат?
а) Документ, подтверждающий личность
б) Документ, подтверждающий права доступа
в) Документ, подтверждающий подлинность ключей
г) Документ, подтверждающий права собственности
14. Какой метод шифрования считается абсолютно надежным?
а) Шифр Цезаря
б) Одноразовый шифр-блокнот
в) Шифр Виженера
г) Асимметричное шифрование
15. Что такое ключ шифра?
а) Секретная информация для шифрования
б) Секретная информация для дешифрования
в) Секретная информация для обеих операций
г) Секретная информация для аутентификации

Экзамен
1. Какой нормативно-правовой акт регулирует защиту персональных данных в России?
а) ФЗ-152
б) ФЗ-98
в) ФЗ-242
г) ФЗ-352
2. Какие методы шифрования относятся к симметричным?
а) Шифр Цезаря
б) RSA
в) Шифр Виженера
г) Эллиптические кривые
3. Что относится к техническим средствам защиты персональных данных?
а) DLP-системы
б) Антивирусное ПО
в) Системы контроля доступа
г) Все вышеперечисленное
4. Какие признаки указывают на возможное заражение троянским ПО?
а) Замедление работы системы
б) Необычное поведение программ
в) Увеличение потребления ресурсов
г) Все вышеперечисленное
5. Какой метод социальной инженерии предполагает создание ложной ситуации?
а) Претекстинг
б) Фишинг
в) Тайпсвотинг
г) Квид про Кво
6. Что такое “дорожное яблоко”?
а) Метод социальной инженерии
б) Вид вредоносного ПО
в) Способ шифрования
г) Метод криптоанализа
7. Какие компоненты входят в систему цифровой подписи?
а) Открытый ключ
б) Закрытый ключ
в) Сертификат
г) Все вышеперечисленное
8. Что обеспечивает абсолютная секретность при правильном использовании?
а) Шифр Цезаря
б) Одноразовый шифр-блокнот
в) Шифр Виженера
г) Асимметричное шифрование
9. Какие характеристики должны быть у современного криптографического протокола?
а) Стойкость к атакам
б) Масштабируемость
в) Простота реализации

г) Все вышеперечисленное
10. Что относится к методам сбора информации из открытых источников?
а) Анализ социальных сетей
б) Изучение публичных баз данных
в) Мониторинг форумов
г) Все вышеперечисленное
11. Какие политики безопасности защищают от вредоносного ПО?
а) Запрет на съемные носители
б) Контроль доступа
в) Мониторинг активности
г) Все вышеперечисленное
12. Что такое атака “человек посередине”?
а) Перехват данных
б) Подмена ключей
в) Фишинг
г) Социальная инженерия
13. Какие методы защиты от фишинга являются наиболее эффективными?
а) Антиспам-фильтры
б) Проверка URL
в) Обучение персонала
г) Все вышеперечисленное
14. Что относится к категории конфиденциальной информации?
а) Персональные данные
б) Коммерческая тайна
в) Служебная тайна
г) Все вышеперечисленное
15. Какие требования предъявляются к стойким паролям?
а) Длина не менее 12 символов
б) Использование разных типов символов
в) Отсутствие словарных слов
г) Все вышеперечисленное

6.5. Примерная тематика курсовых работ (проектов)

Учебным планом не предусмотрено

6.6. Методические указания для обучающихся по освоению дисциплины (модуля)

Методические рекомендации по подготовке к лекционным занятиям

Просмотрите конспект сразу после занятий. Пометьте материал конспекта лекций, который вызывает затруднения для понимания. Попытайтесь найти ответы на затруднительные вопросы, используя предлагаемую литературу. Если самостоятельно не удалось разобраться в материале, сформулируйте вопросы и обратитесь на текущей консультации или на ближайшей лекции за помощью к преподавателю. Каждую неделю рекомендуется отводить время для повторения пройденного материала, проверяя свои знания, умения и навыки по контрольным вопросам.
Работа с рекомендованной литературой:
При работе с основной и дополнительной литературой целесообразно придерживаться такой последовательности. Сначала прочитать весь заданный текст в быстром темпе. Цель такого чтения заключается в том, чтобы создать общее представление об изучаемом материале, понять общий смысл прочитанного. Затем прочитать вторично, более медленно, чтобы в ходе чтения понять и запомнить смысл каждой фразы, каждого положения и вопроса в целом. Чтение приносит пользу и становится продуктивным, когда сопровождается записями. Это может быть составление плана прочитанного текста, тезисы или выписки, конспектирование и др. Выбор вида записи зависит от характера изучаемого материала и целей работы с ним. Если содержание материала несложное, легко усваиваемое, можно ограничиться составлением плана. Если материал содержит новую и трудно усваиваемую информацию, целесообразно его законспектировать. План – это схема прочитанного материала, перечень вопросов, отражающих структуру и последовательность материала. Конспект – это систематизированное, логичное изложение материала источника. Различаются четыре типа конспектов: - план-конспект – это развернутый детализированный план, в котором по наиболее сложным вопросам даются подробные пояснения, - текстуальный конспект – это воспроизведение наиболее важных положений и фактов источника, - свободный конспект – это четко и кратко изложенные основные положения в результате глубокого изучения материала, могут присутствовать выписки, цитаты, тезисы; часть материала может быть представлена планом, - тематический конспект – составляется на основе изучения ряда источников и дает ответ по изучаемому вопросу. В процессе изучения материала источника и составления конспекта нужно обязательно применять различные выделения, подзаголовки, создавая блочную структуру конспекта. Это делает конспект легко воспринимаемым и удобным для работы.

Методические рекомендации по подготовке к практическим занятиям

Практические занятия представляют особую форму сочетания теории и практики. Их назначение – углубление проработки теоретического материала предмета путем регулярной и планомерной самостоятельной работы студентов на протяжении всего курса. Процесс подготовки к практическим занятиям включает изучение нормативных документов, обязательной и дополнительной литературы по рассматриваемому вопросу. Непосредственное проведение практического занятия

предполагает, например:
- индивидуальные выступления студентов с сообщениями по какому-либо вопросу изучаемой темы;
- фронтальное обсуждение рассматриваемой проблемы, обобщения и выводы;
- решение задач и упражнений по образцу;
- решение вариантных задач и упражнений;
- решение ситуационных производственных (профессиональных) задач;
- проектирование и моделирование разных видов и компонентов профессиональной деятельности;
- выполнение контрольных работ;
- работу с тестами.
При подготовке к практическим занятиям студентам рекомендуется: внимательно ознакомиться с тематикой практического занятия; прочесть конспект лекции по теме, изучить рекомендованную литературу; составить краткий план ответа на каждый вопрос практического занятия; проверить свои знания, отвечая на вопросы для самопроверки; если встретятся незнакомые термины, обязательно обратиться к словарю и зафиксировать их в тетради. Все письменные задания выполнять в рабочей тетради. Практические занятия развивают у студентов навыки самостоятельной работы по решению конкретных задач.

Методические рекомендации по подготовке к лабораторным работам

Лабораторные работы представляют одну из форм освоения теоретического материала с одновременным формированием практических навыков в изучаемой дисциплине (модуле). Их назначение – углубление проработки теоретического материала, формирование практических навыков путем регулярной и планомерной самостоятельной работы студентов на протяжении всего курса. Процесс подготовки к лабораторным работам включает изучение нормативных документов, обязательной и дополнительной литературы по рассматриваемому вопросу. Непосредственное проведение лабораторной работы предполагает:
- изучение теоретического материала по теме лабораторной работы (по вопросам изучаемой темы);
- выполнение необходимых расчетов и экспериментов;
- оформление отчета с заполнением необходимых таблиц, построением графиков, подготовкой выводов по проделанным экспериментам и теоретическим расчетам;
- по каждой лабораторной работе проводится контроль: проверяется содержание отчета, проверяется усвоение теоретического материала.
Контроль усвоения теоретического материала является индивидуальным.

Методические указания по выполнению отчёта к лабораторным работам

Основным требованием по выполнению лабораторных и практических работ является полное исчерпывающее описание всей проделанной работы, позволяющее судить о полученных результатах, степени выполнения и профессиональной подготовки студентов.
Методические указания обеспечивают комплексный подход в учебной работе студентов, единство и преемственность требований к оформлению результатов работы на разных этапах обучения. С единых позиций приведены основные требования к структуре, оформлению и содержанию отчета по лабораторным и практическим работам.
Структура отчёта:
- цель работы;
- краткие теоретические сведения;
- ход выполнения работы;
- выводы.
Дополнительные элементы:
- приложения;
- библиографический список.
Требования к содержанию отчёта:
1. Титульный лист
В верхнем поле листа указывают полное наименование учебного заведения.
В среднем поле указывается вид работы, в данном случае лабораторная или практическая работа с указанием курса, по которому она выполнена, и ниже ее название. Название работы приводится без слова "тема" и в кавычки не заключается.
Далее ближе к правому краю титульного листа указывают фамилию, инициалы и группу учащегося, выполнившего работу, а также фамилию, инициалы преподавателя, принявшего работу.
В нижнем поле листа указывается место выполнения работы и год ее написания (без слова год).
2. Цель работы должна отражать тему работы, а также конкретные задачи, поставленные студенту на период выполнения работы. По объему цель работы в зависимости от сложности и многозадачности работы составляет от нескольких строк до 0,5 страницы.
3. Краткие теоретические сведения. В этом разделе излагается краткое теоретическое описание изучаемой в работе темы. Материал раздела не должен копировать содержание методического пособия или учебника по данной теме, а ограничивается изложением основных понятий, требующихся для дальнейшей обработки полученных результатов. Объем литературного обзора не должен превышать 1/3 части всего отчета.
4. Ход выполнения работы. В данном разделе подробно излагается методика выполнения работы, процесс получения данных и способ их обработки. Если используются стандартные пакеты компьютерных программ для обработки экспериментальных результатов, то необходимо обосновать возможность и целесообразность их применения, а также подробности обработки данных с их помощью.
5. Выводы по работе - кратко излагаются результаты работы, полученные в результате выполнения работы, а также краткий анализ полученных результатов.

Отчет по лабораторной работе оформляется на листе формата А4. Допускается оформление отчета по лабораторной работе в электронном виде средствами Microsoft Office. Текст работы должен быть напечатан через полтора интервала шрифтом Times New Roman, кегль – 12. Поля должны оставаться по всем четырем сторонам печатного листа: левое – не менее 30 мм, правое – не менее 10, нижнее – не менее 20 и верхнее – не 15 мм.
Для защиты лабораторной работы студент должен подготовить отчет, провести самостоятельную работу, иметь отметку о проверенном отчете.
Результаты определяются по пятибалльной системе оценок.

Методические рекомендации по выполнению реферата

Реферат – письменная работа объемом 8–10 страниц. Это краткое и точное изложение сущности какого-либо вопроса, темы. Тему реферата студент выбирает из предложенных преподавателем или может предложить свой вариант. В реферате нужны развернутые аргументы, рассуждения, сравнения. Содержание темы излагается объективно от имени автора. Функции реферата: информативная, поисковая, справочная, сигнальная, коммуникативная. Степень выполнения этих функций зависит от содержательных и формальных качеств реферата и для каких целей их использует. Требования к языку реферата: должен отличаться точностью, краткостью, ясностью и простотой.
Структура реферата:
1. Титульный лист
2. Оглавление (на отдельной странице). Указываются названия всех разделов (пунктов плана) реферата и номера страниц, указывающие начало этих разделов в тексте реферата.
3. Введение. Аргументируется актуальность исследования, т.е. выявляется практическое и теоретическое значение данного исследования. Далее констатируется, что сделано в данной области предшественниками, перечисляются положения, которые должны быть обоснованы. Обязательно формулируются цель и задачи реферата.
4. Основная часть. Подчиняется собственному плану, что отражается в разделении текста на главы, параграфы, пункты. План основной части может быть составлен с использованием различных методов группировки материала. В случае если используется чья-либо неординарная мысль, идея, то обязательно нужно сделать ссылку на того автора, у кого взят данный материал.
5. Заключение. Последняя часть научного текста. В краткой и сжатой форме излагаются полученные результаты, представляющие собой ответ на главный вопрос исследования.
6. Приложение. Может включать графики, таблицы, расчеты.
7. Библиография (список литературы). Указывается реально использованная для написания реферата литература. Названия книг располагаются по алфавиту с указанием их выходных данных. Общие требования к построению, содержанию и оформлению».
При проверке реферата оцениваются:
- знание фактического материала, усвоение общих представлений, понятий, идей;
- характеристика реализации цели и задач исследования;
- степень обоснованности аргументов и обобщений;
- качество и ценность полученных результатов;
- использование литературных источников;
- культура письменного изложения материала;
- культура оформления материалов работы.
Правила написания научных текстов (реферат):
Здесь приводятся рекомендации по консультированию студентов относительно данного вида самостоятельной работы. Во время консультаций руководителю следует предложить к обсуждению следующие вопросы.
• Какова истинная цель Вашего научного текста – это поможет Вам разумно распределить свои силы и время.
• Важно разобраться, кто будет «читателем» Вашей работы.
• Начинать писать серьезную работу следует не раньше, чем возникнет ощущение, что по работе с источниками появились идеи, которыми можно поделиться.
• Должна быть идея, а для этого нужно научиться либо относиться к разным явлениям и фактам несколько критически (своя идея – как иная точка зрения), либо научиться увлекаться какими-то известными идеями, которые нуждаются в доработке (идея – как оптимистическая позиция и направленность на дальнейшее совершенствование уже известного).
• Писать следует ясно и понятно, стараясь основные положения формулировать четко и недвусмысленно, а также стремясь структурировать свой текст.
• Объем текста и различные оформительские требования во многом зависят от принятых в конкретном учебном заведении порядков.

Методические рекомендации по выполнению контрольных работ

Контрольная работа выполняется по вариантам. На бланке указывается факультет, курс, группа, ФИО студента. Вопросы строятся на основе тестовых и ситуативных заданий. В тестовых заданиях, выбирается правильный(ые) ответ(ы). При решении ситуативных заданий выбирается правильная последовательность действий в рассматриваемой ситуации.
Проверка контрольной работы позволяет выявить и исправить допущенные студентами ошибки, указать, какие вопросы дисциплины (модуля) ими недостаточно усвоены и требуют доработки. Студент должен внимательно ознакомиться с письменными замечаниями преподавателя и приступить к их исправлению, для чего еще раз повторить соответствующий материал.

Методические рекомендации по подготовке к коллоквиуму

Коллоквиумом называется собеседование преподавателя и студента по заранее определенным контрольным вопросам.

Целью коллоквиума является формирование у студента навыков анализа теоретических проблем на основе самостоятельного изучения учебной и научной литературы. На коллоквиум выносятся крупные, проблемные, нередко спорные теоретические вопросы. Упор делается на монографические работы профессора-автора данного спецкурса. От студента требуется:
- владение изученным в ходе учебного процесса материалом, относящимся к рассматриваемой проблеме;
- знание разных точек зрения, высказанных в научной литературе по соответствующей проблеме, умение сопоставлять их между собой;
- наличие собственного мнения по обсуждаемым вопросам и умение его аргументировать.
Коллоквиум - это не только форма контроля, но и метод углубления, закрепления знаний студентов, так как в ходе собеседования преподаватель разъясняет сложные вопросы, возникающие у студента в процессе изучения данного источника. Однако коллоквиум не консультация и не экзамен. Его задача добиться глубокого изучения отобранного материала, пробудить у студента стремление к чтению дополнительной социологической литературы. Подготовка к коллоквиуму начинается с установочной консультации преподавателя, на которой он разъясняет развернутую тематику проблемы, рекомендует литературу для изучения и объясняет процедуру проведения коллоквиума. Как правило, на самостоятельную подготовку к коллоквиуму студенту отводится 3-4 недели. Методические указания состоят из рекомендаций по изучению источников и литературы, вопросов для самопроверки и кратких конспектов ответа с перечислением основных фактов и событий, относящихся к пунктам плана каждой темы. Это должно помочь студентам целенаправленно организовать работу по овладению материалом и его запоминанию. При подготовке к коллоквиуму следует, прежде всего, просмотреть конспекты лекций и практических занятий и отметить в них имеющиеся вопросы коллоквиума. Если какие-то вопросы вынесены преподавателем на самостоятельное изучение, следует обратиться к учебной литературе, рекомендованной преподавателем в качестве источника сведений.
Коллоквиум проводится в форме индивидуальной беседы преподавателя с каждым студентом или беседы в небольших группах (2-3 человека). Обычно преподаватель задает несколько кратких конкретных вопросов, позволяющих выяснить степень добросовестности работы с литературой, проверяет конспект. Далее более подробно обсуждается какая-либо сторона проблемы, что позволяет оценить уровень понимания. По итогам коллоквиума выставляется дифференцированная оценка по пятибалльной системе.

Методические рекомендации по устному опросу/самоподготовке

После изучения определенной темы по записям в конспекте и учебнику, а также решения достаточного количества соответствующих задач на практических занятиях и самостоятельно студенту рекомендуется, используя лист опорных сигналов,
воспроизвести по памяти определения, выводы формул, формулировки основных положений и доказательств. В случае необходимости следует рекомендовать еще раз внимательно разобраться в материале. Иногда недостаточность усвоения того или иного вопроса выясняется только при изучении дальнейшего материала. В этом случае надо вернуться назад и повторить плохо усвоенный материал. Важный критерий усвоения теоретического материала – умение решать задачи или пройти тестирование по пройденному материалу. Однако преподавателю следует помнить, что правильное решение задачи может получиться в результате применения механически заученных формул без понимания сущности теоретических положений.

Методические рекомендации по подготовке к семинарским занятиям

Одним из видов внеаудиторной самостоятельной работы является подготовка к семинарским занятиям. Семинар – форма учебно-практических занятий, при которой студенты обсуждают сообщения, доклады и рефераты, выполненные ими по результатам учебных или научных исследований под руководством преподавателя. Преподаватель в этом случае является координатором обсуждений темы семинара, подготовка к которому является обязательной. Поэтому тема семинара и основные источники обсуждения предъявляются до обсуждения для детального ознакомления, изучения. Цели обсуждений направлены на формирование навыков профессиональной полемики и закрепление обсуждаемого материала. Семинар – это такая форма организации обучения, при которой на этапе подготовки доминирует самостоятельная работа учащихся с учебной литературой и другими дидактическими средствами над серией вопросов, проблем и задач, а в процессе семинара идут активное обсуждение, дискуссии и выступления учащихся, где они под руководством преподавателя делают обобщающие выводы и заключения. Семинар предназначен для углубленного изучения дисциплины, овладения методологией научного познания, то главная цель семинарских занятий – обеспечить студентам возможность овладеть навыками и умениями использования теоретического знания применительно к особенностям изучаемой отрасли.

Методические рекомендации по подготовке к эссе

Одним из видов самостоятельной работы студентов является написание творческой работы по заданной либо согласованной с преподавателем теме. Творческая работа (эссе) представляет собой оригинальное произведение объемом 500-700 слов, посвященное какой-либо значимой классической либо современной проблеме в определенной теоретической и практической области. Творческая работа не является рефератом и не должна носить описательный характер, большое место в ней должно быть уделено аргументированному представлению своей точки зрения студентами, критической оценке рассматриваемого материала и проблематики, что должно способствовать раскрытию творческих и аналитических способностей. Цели написания эссе – научиться логически верно и аргументировано строить устную и письменную речь; работать над углублением и систематизацией своих философских знаний; овладеть способностью использовать основы знаний для формирования мировоззренческой позиции. Приступая к написанию эссе, изложите в одном предложении, что именно вы будете утверждать и доказывать (свой тезис).

Методические рекомендации по подготовке к докладу

Для подготовки доклада необходимо выбрать актуальную тему. Желательно, чтобы тема была интересна докладчику и вызывала желание качественно подготовить материалы. Подготовка доклада предполагает: определение цели доклада; подбор необходимого материала, определяющего содержание доклада; составление плана доклада, распределение собранного материала в необходимой логической последовательности.
Композиция доклада имеет вступление, основную часть и заключение.
Вступление должно содержать: название доклада; сообщение основной идеи; современную оценку предмета изложения; краткое перечисление рассматриваемых вопросов; интересную для слушателей форму изложения. Основная часть, в которой необходимо раскрыть суть темы, обычно строится по принципу отчёта. Задача основной части: представить достаточно данных для того, чтобы слушатели заинтересовались темой.
Заключение – чёткое обобщение и краткие выводы по излагаемой теме.

Методические рекомендации по подготовке к собеседованию

Собеседование – средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п.
Цель собеседования: проверка усвоения знаний; умений применять знания; сформированности профессионально значимых личностных качеств.
Подготовка к собеседованию предполагает повторение пройденного материала и приобретение навыка свободного владения терминологией и фактическими данными по определенному разделу дисциплины (модуля).

Методические рекомендации по подготовке к тестированию/ итоговому тестированию

Тестирование/итоговое тестирование – это система стандартизированных заданий, определенного содержания и упорядоченных в рамках определенной стратегии предъявления, позволяющая качественно оценить структуру и эффективно измерить уровень знаний, умений и навыков по дисциплине (модулю). Тестирование позволяет оценить у студентов уровень знаний фактического материала, умения логически мыслить, способности к рефлексии и творческому подходу к решению поставленной задачи на каждом этапе их обучения.
При самостоятельной подготовке к тестированию студенту необходимо:
- четко выяснить все условия тестирования заранее (сколько тестов будет предложено, сколько времени отводится на тестирование, какова система оценки результатов);
- проконсультироваться с преподавателем по вопросу выбора учебной литературы;
- проработать информационный материал по разделу дисциплине;
- конспективно выписать из соответствующих разделов учебной дисциплины основные понятия, ключевые идеи, теоретические концепции и подходы;
- повторить теоретический материал лекций, самостоятельно изученной учебной и научной литературы, семинарских занятий.
При выполнении тестовых заданий рекомендуется:
- внимательно полностью прочитать вопрос и предлагаемые варианты ответов, выбрать правильные из них (их может быть несколько);
- при затруднении при ответе на сложный для студента вопрос целесообразно переходить к другим вопросам теста. По завершению ответов на все последующие вопросы теста необходимо вернуться к трудному вопросу и дать на него продуманный ответ;
- по окончании тестирования следует проверить правильность данных ответов на вопросы теста, чтобы избежать механических ошибок.

Методические рекомендации по подготовке к экзамену

Изучение многих общепрофессиональных и специальных дисциплин завершается экзаменом. Подготовка к экзамену способствует закреплению, углублению и обобщению знаний, получаемых, в процессе обучения, а также применению их к решению практических задач. Готовясь к экзамену, студент ликвидирует имеющиеся пробелы в знаниях, углубляет, систематизирует и упорядочивает свои знания. На экзамене студент демонстрирует то, что он приобрел в процессе обучения по конкретной дисциплине (модулю). Экзаменационная сессия – это серия экзаменов, установленных учебным планом. Между экзаменами интервал 2-4 дня, в течение студент систематизирует уже имеющиеся знания. На консультации перед экзаменом студенты должны быть ознакомлены с основными требованиями и получить ответы на возникающие в процессе подготовки
вопросы. Необходимо ориентировать студентов на систематическую подготовку к занятиям в течение семестра, что позволит использовать время экзаменационной сессии для
систематизации знаний.

Методические рекомендации по подготовке к зачету/зачету с оценкой

В ходе подготовки к зачету/зачету с оценкой студент, в первую очередь, должен систематизировать знания, полученные в ходе изучения дисциплины. К зачету/зачету с оценкой необходимо готовиться целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине (модулю). В самом начале учебного курса познакомьтесь со следующей учебно-методической документацией:
- программой дисциплины (модуля);
- перечнем знаний, умений и навыков, которыми студент должен владеть;

- тематическими планами лекций, семинарских занятий;
- учебниками, учебными пособиями по дисциплине, а также электронными ресурсами;
- перечнем вопросов к зачету/зачету с оценкой.

После этого у обучающихся должно сформироваться четкое представление об объеме и характере знаний и умений, которыми надо будет овладеть по дисциплине (модулю). Систематическое выполнение учебной работы на лекциях и лабораторных занятиях позволит успешно освоить дисциплину (модуль) и создать хорошую базу для сдачи зачета/зачета с оценкой.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Рекомендуемая литература	
7.1.1. Основная литература	
Л.1.1	Бабаш А.В., Баранова Е.К., Мельников Ю.Н. Информационная безопасность. Лабораторный практикум + еПриложение [Электронный ресурс]:Учебное пособие. - Москва: КноРус, 2023. - 131 с. – Режим доступа: https://book.ru/book/949452
Л.1.2	Мельников В.П., Куприянов А.И., Васильева Т.Ю., Мельников В.П. Информационная безопасность [Электронный ресурс]:Учебник. - Москва: КноРус, 2023. - 371 с. – Режим доступа: https://book.ru/book/950148
Л.1.3	Медведев В.А. Информационная безопасность. Введение в специальность + еПриложение:Тесты [Электронный ресурс]:Учебник. - Москва: КноРус, 2023. - 143 с. – Режим доступа: https://book.ru/book/948870
Л.1.4	Медведев В.А. Информационная безопасность. Введение в специальность + еПриложение:Тесты [Электронный ресурс]:Учебник. - Москва: КноРус, 2024. - 143 с. – Режим доступа: https://book.ru/book/951878
Л.1.5	Прохорова О. В. Информационная безопасность и защита информации [Электронный ресурс]:учебник для вузов. - Санкт-Петербург: Лань, 2023. - 124 с. – Режим доступа: https://e.lanbook.com/book/293009
Л.1.6	Ищейнов В.Я. Информационная безопасность и защита информации: словарь терминов и понятий [Электронный ресурс]:Словарь. - Москва: Русайнс, 2024. - 226 с. – Режим доступа: https://book.ru/book/951881
7.1.2. Дополнительная литература	
Л.2.1	Никифоров С. Н. Методы защиты информации. Шифрование данных [Электронный ресурс]:учебное пособие. - Санкт-Петербург: Лань, 2019. - 160 с. – Режим доступа: https://e.lanbook.com/book/114699
7.2. Лицензионное и свободно распространяемое программное обеспечение в том числе отечественного производства	
7.2.1	Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition
7.2.2	Microsoft Windows 10 Pro
7.2.3	Microsoft Office 2013 Pro Plus
7.2.4	Информационно-поисковая правовая справочная система «Гарант»
7.3. Перечень профессиональных баз данных, информационных справочных систем и ресурсов сети Интернет	
7.3.1	Электронно-библиотечная система "Лань". Режим доступа: https://e.lanbook.com/
7.3.2	Электронно-библиотечная система "Университетская библиотека онлайн". Режим доступа: https://biblioclub.ru/
7.3.3	Электронно-библиотечная система "BOOK.ru". Режим доступа: https://book.ru/
7.3.4	Электронно-библиотечная система "Университетская библиотека онлайн". Режим доступа: https://biblioclub.ru/
7.3.5	Электронно-библиотечная система "Лань". Режим доступа: https://e.lanbook.com/
7.3.6	ПЛАТФОРМА ОНЛАЙН-ОБРАЗОВАНИЯ «РАЗУМ». Режим доступа: https://razoom.mgutm.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

8.1	Адрес: 215119, Смоленская область, Вяземский район, город Вязьма, ул. Ленина, д. 77: аудитория 18-1310 - Лаборатория Учебная аудитория для проведения занятий лекционного типа; занятий семинарского типа, лабораторных и практических занятий; для курсового проектирования (выполнения курсовых работ); для проведения групповых и индивидуальных консультаций; для текущего контроля и промежуточной аттестации : Рабочие места обучающихся; Рабочее место преподавателя; Классная доска; 15 рабочих мест обучающихся оснащенные ПЭВМ с подключением к сети интернет и обеспечением доступа в электронную информационно-образовательную среду; Ноутбук переносной; Переносной проектор; Переносной экран; Учебно-наглядные пособия
8.2	Адрес: 215119, Смоленская область, Вяземский район, город Вязьма, ул. Ленина, д. 77: аудитория 18-1303 - Лаборатория Учебная аудитория для проведения занятий лекционного типа; занятий семинарского типа, лабораторных и практических занятий; для курсового проектирования (выполнения курсовых работ); для проведения групповых и индивидуальных консультаций; для текущего контроля и промежуточной аттестации : Рабочие места обучающихся; Рабочее место преподавателя; Классная доска; 11 рабочих мест обучающихся, оснащенных ПЭВМ с подключением к сети интернет и обеспечением доступа в электронную информационно-образовательную среду; Комплект типового лабораторного оборудования на основе программируемого контроллера АПК1-С-К; Комплект типового лабораторного оборудования ОАП1-С-Р; макет автоматизированной системы «Умное кафе», образовательный набор по электронике, робототехнике и микропроцессорной технике.

9. ОРГАНИЗАЦИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Организация образовательного процесса для лиц с ограниченными возможностями здоровья осуществляется в соответствии с «Методическими рекомендациями по организации образовательного процесса для инвалидов и лиц с

ограниченными возможностями здоровья в образовательных организациях высшего образования, в том числе оснащенности образовательного процесса» Министерства образования и науки РФ от 08.04.2014г. № АК-44/05вн. В образовательном процессе используются социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе. Студенты с ограниченными возможностями здоровья, в отличие от остальных студентов, имеют свои специфические особенности восприятия, переработки материала. Подбор и разработка учебных материалов производится с учетом индивидуальных особенностей. Предусмотрена возможность обучения по индивидуальному графику, при составлении которого возможны различные варианты проведения занятий: в академической группе и индивидуально, на дому с использованием дистанционных образовательных технологий.

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы
Руководитель ОПОП
_____

Рабочая программа актуализирована, обсуждена и одобрена на заседании обеспечивающей кафедры
Системной автоматизации и информационных технологий
Протокол от __ _____ 2027 г. № __
Зав. кафедрой Кузьмин Константин Анатольевич_____

Рабочая программа согласована на заседании выпускающей кафедры
Системной автоматизации и информационных технологий
Протокол от __ _____ 2027 г. № __
Зав. кафедрой Кузьмин Константин Анатольевич _____

==========

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы
Руководитель ОПОП
_____

Рабочая программа актуализирована, обсуждена и одобрена на заседании обеспечивающей кафедры
Системной автоматизации и информационных технологий
Протокол от __ _____ 2028 г. № __
Зав. кафедрой Кузьмин Константин Анатольевич_____

Рабочая программа согласована на заседании выпускающей кафедры
Системной автоматизации и информационных технологий
Протокол от __ _____ 2028 г. № __
Зав. кафедрой Кузьмин Константин Анатольевич _____

==========

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы
Руководитель ОПОП
_____

Рабочая программа актуализирована, обсуждена и одобрена на заседании обеспечивающей кафедры
Системной автоматизации и информационных технологий
Протокол от __ _____ 2029 г. № __
Зав. кафедрой Кузьмин Константин Анатольевич_____

Рабочая программа согласована на заседании выпускающей кафедры
Системной автоматизации и информационных технологий
Протокол от __ _____ 2029 г. № __
Зав. кафедрой Кузьмин Константин Анатольевич _____

==========

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы
Руководитель ОПОП
_____

Рабочая программа актуализирована, обсуждена и одобрена на заседании обеспечивающей кафедры
Системной автоматизации и информационных технологий
Протокол от __ _____ 2030 г. № __
Зав. кафедрой Кузьмин Константин Анатольевич_____

Рабочая программа согласована на заседании выпускающей кафедры
Системной автоматизации и информационных технологий
Протокол от __ _____ 2030 г. № __
Зав. кафедрой Кузьмин Константин Анатольевич _____