МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Кузбасский гуманитарно-педагогический институт
федерального государственного бюджетного образовательного учреждения
высшего образования
«Кемеровский государственный университет»

Факультет информатики, математики и экономики

УТВЕРЖДАЮ

Декан А.В. Фомина
«10» февраля 2022 г.

Рабочая программа дисциплины

Б1.Б.20 Методы и средства защиты информации
Направление подготовки

09.03.01 Информатика и вычислительная техника

Направленность (профиль) подготовки
Автоматизированные системы обработки информации и управления

Программа академического бакалавриата

Квалификация выпускника
Бакалавр

Форма обучения
очная, заочная

Год набора 2018

Новокузнецк 2022

СОДЕРЖАНИЕ

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

В результате освоения ООП бакалавриата обучающийся должен овладеть следующими результатами обучения по дисциплине в таблице 1 :

Таблице 1 – Результаты обучения по дисциплине / модулю

Код компетенции по ФГОС	**Результаты освоения ООП** *Содержание*	**Перечень планируемых результатов обучения по дисциплине**
ОПК-5 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Знать: - объекты, виды и стандартные задачи профессиональной деятельности; - квалификационные требования к овладеваемой профессии; - понятие и компоненты информационной и библиографической культуры; - виды и организацию информационных ресурсов и информационных услуг; - базовые понятия информатики и информационно-коммуникационных технологий; - современные тенденции развития информатики и вычислительной техники, компьютерных технологий и пути их применения в профессиональной деятельности; - фундаментальные законы природы и основные физические законы в области механики, термодинамики, электричества и магнетизма, атомной физики; - основы алгебры и геометрии, математического анализа, теории вероятностей и математической статистики, дискретной математики, на уровне, необходимом для решения стандартных задач профессиональной деятельности; - виды угроз, возникающие в процессе информационной деятельности; - методы и средства обеспечения информационной безопасности объектов профессиональной деятельности. Уметь: - применять методы алгебры и геометрии, математического анализа, теории вероятностей и математической статистики, дискретной математики, физические законы, основные методы информатики и информационно-коммуникационные технологии, для решения практических задач профессиональной деятельности; - проводить наиболее рациональным способом профессионально-ориентированный поиск информации в различных ресурсах с применением информационно-коммуникационных технологий в соответствии с поставленными задачами; - составлять и оформлять в соответствии с действующими стандартами	Знать: – виды угроз, возникающие в процессе информационной деятельности; – методы и средства обеспечения информационной безопасности объектов профессиональной деятельности. Уметь: – выявлять угрозы информационной безопасности; – анализировать и выбирать методы и средства обеспечения информационной безопасности. Владеть: методами и средствами обеспечения информационной безопасности объектов профессиональной деятельности.

	библиографическое описание документов; - выявлять угрозы информационной безопасности; - анализировать и выбирать методы и средства обеспечения информационной безопасности. Владеть: - представлениями о системе общепрофессиональных знаний, способствующих выполнению профессиональных действий; - навыками осмысления, систематизации, интерпретации профессиональных задач в области огладываемой профессиональной деятельности; - информационной и библиографической культурой для решения задач профессиональной деятельности; - понятийным аппаратом информатики; - современными программными средствами решения практических задач; - элементами функционального анализа, численными методами решения систем дифференциальных уравнений; - методами теории вероятностей и математической статистики; - методами математической логики, теории графов и теории алгоритмов; - численными методами решения систем алгебраических уравнений, методами аналитической геометрии; - основными теоретическими и экспериментальными методами физических исследований и математического моделирования физических процессов. - методами и средствами обеспечения информационной безопасности объектов профессиональной деятельности.	

2. Место дисциплины в структуре ООП бакалавриата

Дисциплина «Защита информации» относится к обязательным дисциплинам ОПОП.

Дисциплина изучается на 4 курсе в 7 семестре при очной форме обучения и на 3 курсе в 6 семестре для заочной..

Дисциплина «Методы и средства защиты информации» участвует в формировании компетенции ОПК-5 совместно с дисциплинами, представленными в таблице 2

Таблица 2 – Структурно-логическая схема формирования компетенций

Предыдущие дисциплины	Последующие дисциплины
Б1.Б.11 Информатика Б1.Б.15 Математика Б1.Б.16 Физика Б1.Б.17 Дискретная математика Б1.Б.18 Теория вероятностей и математическая статистика Б1.В.01 Введение в профессиональную деятельность Б2.В.01(У) Учебная практика. Практика по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности ФТД.02 Выравнивающий курс математики	Б3.Б.01(Д) Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты

3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины (модуля) составляет 3 зачетные единицы (ЗЕТ), 108 (академических часов.

3.1. Объём дисциплины (модуля) по видам учебных занятий (в часах)

Объём дисциплины	**Всего часов**	
	для очной формы обучения	для заочной формы обучения
Общая трудоемкость дисциплины	108	108
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	62	14
Аудиторная работа (всего):	62	14
в т. числе:		
Лекции	18	6
Семинары, практические занятия		
Практикумы	44	8
Лабораторные работы		
Внеаудиторная работа (всего):		
В том числе, индивидуальная работа обучающихся с преподавателем:		
Курсовое проектирование		
Контрольная работа		
Творческая работа (эссе)		
Самостоятельная работа обучающихся (всего)	46	90
Вид промежуточной аттестации обучающегося – зачет		4

4. Содержание дисциплины, структурированное по темам с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Разделы дисциплины (модуля) и трудоемкость по видам учебных занятий (в академических часах)

для очной формы обучения

№ п/п	Раздел дисциплины	Общая трудоёмкость *(часах)*	Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость (в часах)			Формы текущего контроля успеваемости
			аудиторные учебные занятия		самостоятельная работа обучающихся	
		всего	лекции	семинары, практические занятия		
1.	Введение в предмет. Угрозы информационной безопасности	14	2	6	6	Устный доклад; отчет по лабораторной работе.
2.	Основные понятия теории информационной безопасности	14	2	6	6	Устный доклад; Отчет по лабораторной работе.
3.	Программно-технические методы защиты	14	2	6	6	Устный доклад; Отчет по лабораторной работе.
4.	Криптографические методы защиты	14	2	6	6	Устный доклад; Отчет по лабораторной работе.
5.	Организационно правовые методы информационной безопасности	16	2	6	8	Устный доклад; Отчет по лабораторной работе.
6.	Роль стандартов в обеспечении информационной безопасности	18	4	6	8	Устный доклад; Отчет по лабораторной работе.
7.	Технологии построения защищенных систем	18	4	8	6	Устный доклад; Отчет по лабораторной работе
Форма контроля						Зачет
ИТОГО		**108**	**18**	**44**	**46**	

для заочной формы обучения

№ п/п	Раздел дисциплины	Общая трудоёмкость *(часах)*	Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость (в часах)			Формы текущего контроля успеваемости
			аудиторные учебные занятия		самостоя-тельная работа обучаю-щихся	
		всего	лек-ции	семинары, практичес-кие занятия		
1.	Введение в предмет. Угрозы информационной безопасности	14	0,5	1	12,5	Устный доклад; отчет по лабора-торной работе.
2.	Основные понятия теории информационной безопасности	14	0,5	1	12,5	Устный доклад; Отчет по лабора-торной работе.
3.	Программно-технические методы защиты	14	1	1	12	Устный доклад; Отчет по лабораторной работе.
4.	Криптографические методы защиты	14	1	1	12	Устный доклад; Отчет по лабора-торной работе.
5.	Организационно правовые методы информационной безопасности	16	1	1	14	Устный доклад; Отчет по лабораторной работе.
6.	Роль стандартов в обеспечении информационной безопасности	16	1	1	14	Устный доклад; Отчет по лабораторной работе.
7.	Технологии построения защищенных систем	16	1	2	13	Устный доклад; Отчет по лабораторной работе
	Форма контроля	4				Зачет
ИТОГО		**108**	**6**	**8**	**90**	

4.2 Содержание дисциплины, структурированное по темам

Содержание лекционного курса

№ п/п	Наименование раздела дисциплины	Содержание
1	Введение в предмет. Угрозы информационной безопасности	Понятие информационной безопасности и защищенной системы. Международные стандарты информационного обмена. Понятие угрозы. Необходимость защиты информационных систем и телекоммуникаций. Технические предпосылки кризиса информационной безопасности. Информационная безопасность в условиях функционирования в России глобальных сетей. Основные задачи обеспечения защиты информации. Основные методы и средства защиты информационных систем. Понятие угрозы. Виды противников или «нарушителей». Виды возможных нарушений информационной системы. Анализ угроз информационной безопасности. Классификация видов угроз информационной безопасности по различным признакам (по природе возникновения, степени преднамеренности и т.п.). Свойства информации: конфиденциальность, доступность, целостность. Угроза раскрытия параметров системы, угроза нарушения конфиденциальности, угроза нарушения целостности, угроза отказа служб. Примеры реализации угроз информационной безопасности. Защита информации. Основные принципы обеспечения информационной безопасности в автоматизированных системах. Причины, виды и каналы утечки информации.
2	Основные понятия теории информационной безопасности	Основные положения теории информационной безопасности информационных систем. Понятие угрозы. Информационная безопасность в условиях функционирования в России глобальных сетей. Формальные модели безопасности их значение для построения защищенных информационных систем. Понятие доступа к данным и монитора безопасности. Функции монитора безопасности. Понятие политики безопасности информационных систем. Разработка и реализация политики безопасности. Управление доступом к данным. Основные типы политики безопасности управления доступом к данным: дискреционная и мандатная политика безопасности. Анализ способов нарушений безопасности. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.
3	Программно-технические методы защиты	Общее представление о структуре защищенной информационной системы. Особенности современных информационных систем, факторы влияющие на безопасность информационной системы. Понятие информационного сервиса безопасности. Виды сервисов безопасности. Идентификация и аутентификация. Парольные схемы аутентификации. Симметричные схемы аутентификации субъекта. Несимметричные схемы аутентификации (с открытым ключом). Аутентификация с третьей доверенной стороной (схема Kerberos). Токены, смарт-карты, их применение. Использование биометрических данных при аутентификации пользователей. Сервисы управления доступом. Механизмы доступа данных в операционных системах, системах управления базами данных. Ролевая модель управления доступом. Протоколирование и аудит. Задачи и функции аудита. Структура

№ п/п	Наименование раздела дисциплины	Содержание
		журналов аудита. Активный аудит, методы активного аудита. Обеспечение защиты корпоративной информационной среды от атак на информационные сервисы. Защита Интернет-подключений, функции и назначение межсетевых экранов. Понятие демилитаризованной зоны. Виртуальные частные сети (VPN), их назначение и использование в корпоративных информационных системах. Защита данных и сервисов от воздействия вредоносных программ. Вирусы, троянские программы. Антивирусное программное обеспечение. Защита системы электронной почты. Спам, борьба со спамом.
4	Криптографические методы защиты	Методы криптографии. Средства криптографической защиты информации (СКЗИ). Криптографические преобразования. Шифрование и дешифрование информации. Причины нарушения безопасности информации при ее обработке СКЗИ (утечки информации по техническому каналу, неисправности в элементах СКЗИ, работа совместно с другими программами). Использование криптографических средств для решения задач идентификация и аутентификация. Электронная цифровая подпись (ЭЦП), принципы ее формирования и использования. Подтверждение подлинности объектов и субъектов нформациионной системы. Контроль за целостностью информации. Хэш-функции, принципы использования хэш-функций для обеспечения целостности данных.
5	Организационно правовые методы информационной безопасности	Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Особенности сертификации и стандартизации криптографических услуг. Законодательная база информационной безопасности. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.
6	Роль стандартов в обеспечении информационной безопасности	Роль стандартов информационной безопасности. Квалификационный анализ уровня безопасности. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности. Критерии безопасности компьютерных систем министерства обороны США (“Оранжевая книга”). Базовые требования безопасности: требования политики безопасности, требования подотчетности (аудита), требования корректности. Классы защищенности компьютерных систем. Интерпретация и развитие Критериев безопасности. Руководящие документы Гостехкомиссии России. Структура требований безопасности. Основные положения концепции защиты средств вычислительной техники от несанкционированного доступа (НСД) к информации. Показатели защищенности средств вычислительной техники от НСД. Классы защищенности автоматизированных систем. Международные стандарты информационной безоапсности. Стандарт ISO/IEC 15408 «Критерии оценки безопасности

№ п/п	Наименование раздела дисциплины	Содержание
		информационных технологий» («Единые критерии»). Основные положения Единых критериев. Функциональные требования и требования доверия. Понятие Профиля защиты и Проекта защиты.
7	Технологии построения защищенных систем	Использование защищенных компьютерных систем. Общие принципы построения защищенных систем. Иерархический метод разработки защищенных систем. Структурный принцип. Принцип модульного программирования. Исследование корректности реализации и верификации автоматизированных систем. Спецификация требований предъявляемых к системе. Основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политике безопасности

Содержание практических занятий

№	Наименование раздела дисциплины	Содержание раздела дисциплины
1	Введение в предмет. Угрозы информационной безопасности	Построение матрицы рисков для выбранного предприятия.
2	Основные понятия теории информационной безопасности	Знакомство с основными направлениями работ в рамках федеральной программы «Электронная Россия», а также со сведениями о порядке использования и действующих алгоритмах постановки ЭЦП.
3	Программно-технические методы защиты	Исследование защиты с применением пароля, а также исследование методов противодействия атакам на пароль.
4	Криптографические методы защиты	Методы современной криптографии на примере программирования одного из предложенных алгоритмов.
5	Организационно правовые методы информационной безопасности	Проведение анализ способов нарушений безопасности на прим.
6	Роль стандартов в обеспечении информационной безопасности	Изучение логики работы и формы предоставления информации сетевыми анализаторами; овладение приемов анализа сетевого трафика; получение базовых знаний для обнаружения и организации сетевых атак.
7	Технологии построения защищенных систем	Составление документа «Политика безопасности»

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Методические указания студенту по организации самостоятельной работы размещены на сайте НФИ КемГУ в разделе «Основные профессиональные образовательные программы высшего образования, реализуемые в НФИ КемГУ/ Методические и иные документы». Ос-новная и дополнительная учебная литература и Интернет-ресурсы, необходимые для выпол-нения самостоятельной работы и теоретического освоения дисциплины по графику представ-лены в разделах 7 и 8 настоящей РПД..

6. Фонд оценочных средств для проведения промежуточной аттестации

6.1 Типовые контрольные задания или иные материалы

а) Типовые вопросы к зачету

Тема 1. Введение в предмет. Угрозы информационной безопасности.

1. Что называется информационной безопасностью?
2. Какие данные называются критическими?
3. Какие вы знаете признаки компьютерных преступлений в интернет технологиях и какие основные технологии, и методы используются при совершении компьютерных преступлений?
4. Какие четыре уровня защиты компьютерных (интернет технологий) и информационных ресурсов вы можете назвать?
5. Перечислите признаки, свидетельствующие о наличии уязвимых мест в информационной безопасности?

Тема 2. Основные понятия теории информационной безопасности.

6. Перечислите меры защиты информационной безопасности?
7. Какие меры предпринимают по защите целостности информации?
8. Какие меры предпринимают по защите системных программ?
9. Дублирование информации и его классы.
10. Перечислите позиции административного уровня.
11. Назовите цель ОНРВ и его основные положения?

Тема 3. Программно-технические методы защиты.

12. Что такое межсетевой экран и какая у него роль в защите.
13. Законодательная основа информационной безопасности, статьи и пр.
14. Что такое политика безопасности на административном уровне?
15. Основные принципы защиты информации на административном уровне?
16. Средства Разграничения доступа.
17. Что такое CGI процедуры, их назначения?
18. Чем опасна программа, полученная из ненадежного источника, какие вы знаете средства контроля над такими программами?
19. Как осуществляется защита WEB-серверов?

Тема 4. Криптографические методы защиты.

20. Криптография и криптоанализ. Назначение криптографии.
21. Перечислите известные алгоритмы шифрования. Цифровые деньги и их характеристики.
22. Симметричная и асимметричная методология шифрования.
23. Криптографические средства защиты.
24. Квантовая криптография и ККС.

Тема 5. Организационно-правовые методы информационной безопасности.

25. Чем определяется концепция обеспечения безопасности АСОИ.
26. В чем состоит избирательная политика безопасности способом управления доступом.
27. Организационные меры безопасности АСОИ.
28. Матрица доступа в АСОИ.
29. Полномочное управление доступом.
30. Избирательное управление доступом.

Тема 6. Роль стандартов в обеспечении информационной безопасности.

31. Что такое универсальная операционная система?
32. Что такое компьютерный вирус.
33. Полиморфные вирусы.
34. Суррогатные платежные средства.
35. Файловые вирусы и алгоритм их работы.
36. Особенность макровирусов.

Тема 7. Технологии построения защищенных систем.

37. Полномочное управление доступом.
38. Избирательное управление доступом.
39. Отказоустойчивые компьютерные системы.
40. Что вы понимаете под технологией RAID.
41. Методы дублирования информации.

б) Типовые практические задания на зачет

Задание 1. Для одноалфавитного метода с задаваемым смешением выполнить шифрование с произвольным смещением.

Задание 2. Для одноалфавитного метода с задаваемым смешением выполнить дешифрование зашифрованный шифром Цезаря текст.

Задание 3. Проверить на простоту два произвольных целых числа разрядностью 5.

Задание 4. Задан интервал вида $[x, x + L]$. Вычислить количество $П(x, L)$ простых чисел в интервале и сравнить с величиной $L/1n(x)$. При каких условиях $П(x, L)/L$ близко к $1/1n(x)$ при заданных $x = 2000$, $L = 500$, количество простых чисел для деления 5-15, количество оснований 1-2?

Задание 5. Найти в интервале (1000, 1000 + 300) все простые числа. Пусть L(i) - разность между двумя соседними простыми числами. Построить гистограмму для $L(i)$. Вычислить выборочное среднее $L_{сред}$. Сравнить с величиной $1n(x)$, где x - середина интервала. Задано: количество простых чисел для деления 5-20, количество оснований 1-3.

Задание 6. Для заданного набора чисел $\{k\}$ оценить относительную погрешность формулы для k-го простого числа:

$p(k) = k/ln(k)$, $k= \{10, 15, 20, 30, 35\}$.

Задание 7. В интервале (500, 500 + 200) построить график относительного количества натуральных чисел, проходящих «решето Эратосфена», т.е. не делящихся на первые к простых. Расчет производится для всех $k <= 10$.

6.2 Оценочные средства текущего контроля

Оценочными средствами являются: устные доклады, отчеты по практическим работам, тест.

Устные доклады

а) Тематика устных докладов

1. Политика информационной безопасности предприятия.
2. Нормативно-правовая база обеспечения информационной безопасности предприятия.
3. Содержание основных законов Российской Федерации в сфере компьютерного права.
4. Законодательная база РФ по вопросам защиты информации.
5. Комплексный подход к обеспечению информационной безопасности.
6. Законодательные и нормативные акты РФ о предпринимательской деятельности.
7. Машинное представление информации.
8. Виды и формы представления информации.
9. Информация как объект права собственности.
10. Информация как коммерческая тайна.
11. Информация как рыночный продукт.
12. Элементы и объекты защиты в АС.
13. Основные виды вирусов и схемы их функционирования.
14. Обнаружение вирусов и меры по защите и профилактике
15. Основные меры защиты от вирусов.
16. Программно-технические меры обеспечения информационной безопасности.
17. Обеспечение информационной безопасности средствами Windows 7.

18. Безопасное хранение данных на основе шифрования.
19. Американский стандарт шифрования данных DES.
20. Стандарт шифрования данных ГОСТ 28147-89.
21. Система цифровой телефонии.
22. Системы шифрования с открытыми ключами.
23. Цифровые подписи на основе шифросистем с открытыми ключами.
24. Комплексный подход к обеспечению информационной безопасности:
25. Механические системы защиты
26. Оборонительные системы
27. Технические средства обеспечения безопасности подвижных объектов
28. Системы охранной сигнализации
29. Защита интеллектуальной собственности в РФ на современном этапе

б) критерии оценивания

Критериями оценивания доклада являются полнота раскрытия темы, степень ее проработанности, последовательность изложения материала; умения студента самостоятельно работать с литературой и информационно-электронными ресурсами, аргументированно и ясно строить речь, эффектно и наглядно представлять содержание результатов своей работы, а также владения навыками дискуссии и публичной защиты результатов своих исследований.

в) описание шкалы оценивания

Устные доклады оцениваются по шкале «зачтено» / «незачтено».

«Зачтено» выставляется в случае, если студент свободно излагает материал по заданному вопросу, опираясь при этом на литературные и другие дополнительные источники, отвечает на дополнительные уточняющие вопросы преподавателя и аудитории студентов, приводит практические примеры, аргументированно отстаивает свою точку зрения; во время доклада использует раздаточный материал и (или) презентацию.

«Незачтено» выставляется в случае, если в изложении наблюдаются значительные пробелы в знании материала и (или) студент не отвечает на дополнительные уточняющие вопросы и (или) не использует иллюстративный материал.

Отчет по практическим работам

а) разделы отчета

- наименование лабораторной работы;
- постановка задачи, исходные данные;
- описание методов и способов решения;
- этапы решения задачи и (или) ее алгоритмическое обеспечение;
- результаты, представленные в виде таблиц, графиков и т.п. с краткими пояснениями;
- выводы.

б) критерии оценивания

Студент должен продемонстрировать:

умения применять математические методы для формализации и решения прикладных задач; строить модели экономических процессов, исследовать их и вырабатывать рекомендации к их применению на практике; организовывать вычислительный эксперимент на компьютере для исследования поведения экономических объектов, систем, процессов;

владение навыками работы с пакетами прикладных программ для моделирования и анализа экономических процессов.

в) описание шкалы оценивания

«Зачтено» выставляется в случае, если студент выполнил в полном объеме лабораторную работу, не допустил ошибок в расчетах, сделал выводы, свободно излагает этапы решения и результаты работы.

«Незачтено» выставляется в случае, если студент не выполнил лабораторную работу, либо

выполнил, но допустил существенные ошибки в расчетах и (или) не сделал выводы, и (или) не может изложить этапы решения и результаты работы.

Тест

а) типовые задания к тесту

Формы тестовых заданий:

- выбор правильных ответов из перечисленных;
- установление правильной последовательности;
- установление соответствия.

б) критерии оценивания

Критерием оценивания теста является количество правильно выполненных тестовых заданий, свидетельствующих о полноте знаний теоретического материала в области экономико-математического моделирования.

в) описание шкалы оценивания

«Отлично» - процент правильно выполненных заданий составляет от 80% до 100.

«Хорошо» - процент правильно выполненных заданий составляет от 60% до 79.

«Удовлетворительно» - процент правильно выполненных заданий составляет от 50% до 59%.

«Неудовлетворительно» - процент правильно выполненных заданий составляет менее 50%.

6.3 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций

Балльно- рейтиноговая система оценки знаний, умений и навыков

Таблица 7 – Шкала и показатели оценивания результатов учебной работы обучающихся по видам в балльно-рейтинговой системе (БРС)

Учебная работа (виды)	Сумма баллов	Виды и результаты учебной работы	Оценка в аттестации	Баллы
Текущая учебная работа в семестре (посещение занятий по расписанию и выполнение заданий)	80	Лекционные занятия (конспект) (18 занятий)	1б. - посещение 1 лекционного занятия	0-18
		Практические занятия (выполнение заданий) (52 занятий)	42/52 б. - посещение 1 практического занятия и выполнение работы на 51-65% 62/52 б. – посещение 1 занятия и существенный вклад на занятии в работу всей группы, самостоятельность и выполнение работы на 85,1-100%	1 - 62
Итого по текущей работе в семестре				51 – 100 (приведенных баллов)
Промежуточная аттестация (зачет)	20	Зачет	10 б. (пороговое значение) 20 б. (максимальное значение)	10 - 20
Итого по промежуточной аттестации (зачету)				51-100 (приведенных баллов (20)
Суммарная оценка по дисциплине: сумма баллов текущей и промежуточной аттестации				51 - 100

Для обучающихся очной формы обучения в текущей учебной работе в семестре (по графику – в период ТО) планируется выполнение контрольных работ, за которые назначаются баллы, включаемые в общий объем баллов за текущую работу в семестре (см. таблицу 7). Обучающемуся по ЗФО задания на контрольные работы выдаются на установочной сессии. Примеры тем / заданий для контрольных работ и порядок их выбора и утверждения приведены в п. 6.1 данной программы.

В промежуточной аттестации оценка выставляется в ведомость в 100-балльной шкале и в буквенном эквиваленте (таблица 10)

Таблица 10 – Соотнесение 100-балльной шкалы и буквенного эквивалента оценки

Сумма набранных баллов	Уровни освоения дисциплины и компетенций	*Экзамен*		*Зачет*
		Оценка	*Буквенный эквивалент*	*Буквенный эквивалент*
86 - 100	Продвинутый	5	отлично	Зачтено
66 - 85	Повышенный	4	хорошо	
51 - 65	Пороговый	3	удовлетворительно	
0 - 50	Первый	2	неудовлетворительно	Не зачтено

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

а) Основная литература

1. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2021. — 201 с. — (Среднее профессиональное образование). - ISBN 978-5-16-016583-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1191479 (дата обращения: 28.02.2021). – Режим доступа: по подписке.

б) Дополнительная литература

2. Васильков, А. В. Безопасность и управление доступом в информационных системах : учебное пособие / А.В. Васильков, И.А. Васильков. — Москва : ФОРУМ : ИНФРА-М, 2020. — 368 с. — (Среднее профессиональное образование). - ISBN 978-5-91134-360-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1082470 (дата обращения: 28.02.2021). – Режим доступа: по подписке.
3. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах: Учебное пособие / В.Ф. Шаньгин. - Москва : ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с.: ил.; . - (Высшее образование). ISBN 978-5-8199-0411-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/402686 (дата обращения: 28.02.2021). – Режим доступа: по подписке.
4. Партыка, Т. Л. Информационная безопасность: Учебное пособие для студентов учреждений среднего проф. обр. / Т.Л. Партыка, И.И. Попов. - 3-е изд., перераб. и доп. - Москва : Форум, 2008. - 432 с.: ил.; . - (Проф. обр.). ISBN 978-5-91134-246-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/167284 (дата обращения: 28.02.2021). – Режим доступа: по подписке.

8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО - ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ», СОВРЕМЕННЫХ ПРОФЕССИОНАЛЬНЫХ БАЗ ДАННЫХ (СПБД) И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ (ИСС) НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Ресурсы информационно - телекоммуникационной сети «интернет»

1. - Новая электронная библиотека – www.newlibrary.ru
2. - Нехудожественная библиотека – www.nehudlit.ru
3. - Университетская информационная система www.uisrussia.ru

Современные профессиональные базы данных (СПБД) и информационные справочные системы (ИСС) по дисциплине

1. CITForum.ru - on-line библиотека свободно доступных материалов по информационным технологиям на русском языке - http://citforum.ru
2. Научная электронная библиотека eLIBRARY.RU – крупнейший российский информационный портал в области науки, технологии, медицины и образования, содержащий рефераты и полные тексты - www.elibrary.ru
3. Единое окно доступа к образовательным ресурсам - http://window.edu.ru/

9. Методические указания для обучающихся по освоению дисциплины

Подготовка к практическим занятиям

При подготовке к практическим занятиям студент должен изучить теоретический материал по теме занятия (использовать конспект лекций, изучить основную литературу, ознакомиться с дополнительной литературой, при необходимости дополнить конспект, делая в нем соответствующие записи из литературных источников). В случае затруднений, возникающих при освоении теоретического материала, студенту следует обращаться за консультацией к преподавателю. Идя на консультацию, необходимо хорошо продумать вопросы, которые требуют разъяснения.

В начале лабораторного занятия преподаватель знакомит студентов с темой, оглашает план проведения занятия, выдает задание. В течение отведенного времени на выполнение работы студент может обратиться к преподавателю за консультацией или разъяснениями. В конце занятия проводится прием выполненных работ: проверка отчета, собеседование со студентом.

Результаты выполнения практических работ оцениваются как текущая работа на «зачтено»/«незачтено».

Подготовка к устному докладу

Доклады делаются по каждой теме с целью проверки теоретических знаний студента, его способности самостоятельно приобретать новые знания, работать с информационными ресурсами и извлекать нужную информацию.

Доклады заслушиваются в начале лабораторного занятия после изучения соответствующей темы. Продолжительность доклада не должна превышать 5 минут. Тему доклада студент выбирает по желанию из предложенного списка.

При подготовке доклада студент должен изучить теоретический материал, используя основную и дополнительную литературу,обязательно составить план доклада (перечень рассматриваемых им вопросов,отражающих структуру и последовательность материала), подготовить раздаточный материал или презентацию. План доклада необходимо предварительно согласовать с преподавателем.

Выступление должно строиться свободно, убедительно и аргументировано. Преподаватель следит, чтобы выступление не сводилось к простому воспроизведению текста, не допускается простое чтение составленного конспекта доклада. Выступающий также должен быть готовым к вопросам аудитории и дискуссии.

Подготовка к тесту

При подготовке к тесту необходимо изучить темы 1-7. С целью оказания помощи студентам при подготовке к тесту преподавателем проводится групповая консультация с целью разъяснения наиболее сложных вопросов теоретического материала.

Методические указания студенту по освоению дисциплины размещены на сайте НФИ КемГУ в разделе «Основные профессиональные образовательные программы высшего образования, реализуемые в НФИ КемГУ/ Методические и иные документы» по адресу: «https://skado.dissw.ru/table».

10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине / модулю, используемого программного обеспечения

Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом, в том числе помещения для самостоятельной работы, с указанием перечня основного оборудования, учебно-наглядных пособий и используемого программного обеспечения	Адрес (местоположение) помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом (в случае реализации образовательной программы в сетевой форме дополнительно указывается наименование организации, с которой заключен договор)
410 Учебная аудитория (мультимедийная) для проведения: - занятий лекционного типа; Специализированная (учебная) мебель: доска меловая, кафедра, моноблоки аудиторные. Оборудование: стационарное - компьютер, экран, проектор. Используемое программное обеспечение: MSWindows (MicrosoftImaginePremium 3 year по сублицензионному договору № 1212/КМР от 12.12.2018 г. до 12.12.2021 г.), LibreOffice (свободно распространяемое ПО), Яндекс.Браузер (отечественное свободно распространяемое ПО). Интернет с обеспечением доступа в ЭИОС.	654079, Кемеровская область, г. Новокузнецк, пр-кт Металлургов, д. 19
501 Компьютерный класс. Учебная аудитория (мультимедийная) для проведения: - занятий семинарского (практического) типа; - групповых и индивидуальных консультаций; - самостоятельной работы; - текущего контроля и промежуточной аттестации. Специализированная (учебная) мебель: доска меловая, кафедра, столы компьютерные, стулья. Оборудование для презентации учебного материала: стационарное - компьютер преподавателя, экран, проектор. Оборудование: стационарное - компьютеры для обучающихся (17 шт.). Используемое программное обеспечение: MS Windows (Microsoft Imagine Premium 3 year по сублицензионному договору № 1212/КМР от 12.12.2018 г. до 12.12.2021 г.), LibreOffice (свободно распространяемое ПО), BloodshedDev C++ 4.9.9.2 (свободно распространяемое ПО), Firefox 14 (свободно распространяемое ПО), Яндекс.Браузер (отечественное свободно распространяемое ПО), Java (бесплатная версия), UML-диаграммы (бесплатная версия), Консультант Плюс (отечественное ПО, договор об инфо поддержке 1.04.2007), Oracle VM VirtualBox (бесплатная версия), Paint.NET (свободно распространяемое ПО). Интернет с обеспечением доступа в ЭИОС.	654079, Кемеровская область, г. Новокузнецк, пр-кт Металлургов, д. 19

Составитель (и): Зайцев В.Н., аспирант,
ведущий специалист отдела автоматизации расчета заработной платы, кадрового и производственного учета
ООО «Синерго Софт Системс»

(*фамилия, инициалы и должность преподавателя (ей)*)