МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«ИРКУТСКИЙГОСУДАРСТВЕННЫЙУНИВЕРСИТЕТ»
ФГБОУ ВО «ИГУ»

Кафедра прикладной информатики и документоведения

УТВЕРЖДАЮ
Декан факультета бизнес-коммуникаций и информатики
_____ В.К. Карнаухова

«25» марта 2022 г.

Рабочая программа дисциплины (модуля)

Наименование дисциплины (модуля) **Б1.В.17. Основы корпоративной безопасности**
(индекс дисциплины по учебному плану, наименование дисциплины (модуля)).

Направление подготовки: **09.03.03 Прикладная информатика**
(код, наименование направления подготовки)

Направленность (профиль) подготовки: **Прикладная информатика в управлении**

Квалификация выпускника – **бакалавр**

Форма обучения: **очно-заочная** *(с использованием электронного обучения и дистанционных образовательных технологий)*
(очная, заочная (с использованием электронного обучения и дистанционных образовательных технологий), очно-заочная (с использованием электронного обучения и дистанционных образовательных технологий *)*

Согласовано с УМК факультета бизнес- коммуникаций и информатики

Протокол № 7 от «16» марта 2022 г.

Председатель _____ В.К. Карнаухова

Рекомендовано кафедрой прикладной информатики и документоведения

Протокол № 8 от «04» марта 2022 г.

и.о.зав. кафедрой _____ А.В. Рохин

Иркутск – 2022

СОДЕРЖАНИЕ

стр.

.

I. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ (МОДУЛЯ)

Цель: является приобретение навыков организации работы с документами в условиях применения автоматизированных технологий их обработки и с учетом основных требований информационной безопасности.

Задачи дисциплины:

– формирование у студентов единого понимания государственной политики в сфере обеспечения безопасности персональных данных, понимания специфики практического применения федерального закона «О персональных данных», основных подзаконных актов, порядка организации и обеспечения защиты персональных данных в организации (учреждении, предприятии);

– сформировать у студентов методически обоснованных подходов к решению практических задач документационного обеспечения во всех сферах управленческой деятельности,

– овладение традиционными технологиями обработки документов в сочетании с внедрением средств компьютерной техники, новейших программных продуктов,

– приобретение навыков «бездокументного» информационного обеспечения, и создания условий безусловной сохранности документной информации на различных видах носителей.

II. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

2.1. Учебная дисциплина (модуль) «Основы корпоративной безопасности» относится к части, формируемой участниками образовательных отношений Блок 1.Дисциплины (модули)

Дисциплина предназначена для закрепления знаний и умений в сфереуправления и отработки практических навыков в области информационной и корпоративной безопасности.

2.2. Для изучения данной учебной дисциплины (модуля) необходимы знания, умения и навыки, формируемые предшествующими дисциплинами:.Информатика

2.3. Перечень последующих учебных дисциплин, для которых необходимы знания, умения и навыки, формируемые данной учебной дисциплиной: выпускная квалификационная работа

III. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс освоения дисциплины направлен на формирование компетенций (элементов следующих компетенций) в соответствии с ФГОС ВО и ОП ВО по данному направлению подготовки:

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Компетенция	Индикаторы компетенций	Результаты обучения
ПК-3 Способность управлять процессами технической поддержки инфокоммуникационных систем и (или) их составляющих	ПК-3.1	Уметь применять системный подход и математические методы в формализации решения прикладных задач разработки программных приложений разработчика программного обеспечения для решения экономических задач
	ПК-3.2	Владеть навыками использования математических, естественнонаучных,

		социально-экономических, инженерных знаний в разработке компьютерных моделей и прототипов программного обеспечения разработчика программного обеспечения для решения экономических задач
	ПК-3.3	Владеть навыками контроля качества выполнения группой специалистов заявок на техническую поддержку инфокоммуникационных систем и (или) их составляющих

IV. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 3 зачетных единицы, 108 часов, 26 часов на экзамен.

Форма промежуточной аттестации: Экзамен

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

очно-заочная форма обучения

№ п/п	Раздел дисциплины/темы	Семестр	Всего часов	Из них практическая подготовка обучающихся	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)				Формы текущего контроля успеваемости; Форма промежуточной аттестации *(по семестрам)*
					Контактная работа преподавателя с обучающимися			Самостоятельная работа	
					Лекции	Семинарские (практические занятия)	Консультации, контроль		
1.	Раздел 1. Основы корпоративной безопасности	6			6	6	6	20	УО
2.	Раздел 2. Управление корпоративной безопасностью в организации	6			10	10	4	20	УО
	Промежуточная аттестация	8							Экзамен
Итого часов			**108**		**16**	**16**	**10**	**40**	**26**

4.2 План внеаудиторной самостоятельной работы обучающихся по дисциплине

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Затраты времени (час.)		
6	Раздел 1. Основы корпоративной безопасностью в организации Раздел 2. Управление корпоративной безопасностью в организации	**Для овладения знаниями**: чтение текста учебного пособия, дополнительной литературы: составление схем и таблиц по тексту, конспектирование текста; выписки из текста; использование аудио- и видеозаписей, компьютер-ной техники и Интернета и др.; **Для закрепления и систематизации знаний**: работа с конспектом лекции; составление плана и тезисов ответа; составление таблиц для систематизации учебного материала; ответы на контрольные вопросы; подготовка сообщений к выступлению на семинаре; **Для формирования умений**: решение ситуационных задач; рефлексивный анализ профессиональных. Подготовка к зачету с оценкой	1-17	40	УО	ЭОС Форлабс
Общая трудоемкость самостоятельной работы по дисциплине (час)				**40**		
Из них объем самостоятельной работы **с использованием электронного обучения и дистанционных образовательных технологий (час)**				**40**		
Бюджет времени самостоятельной работы, предусмотренный учебным планом для данной дисциплины (час)				**40**		

4.3 Содержание учебного материала

Трудоемкость дисциплины (з.е.)	3
Наименование основных разделов (модулей)	**Раздел 1. Основы корпоративной безопасности** Тема 1. Корпоративная безопасность: понятие и элементы Понятие корпоративной безопасности. Основные составляющие корпоративной безопасности. Важность и сложность проблемы корпоративной безопасности. Законодательный уровень корпоративной безопасности. Обзор российского законодательства в области корпоративной безопасности. Тема 2. Типы противоправного поведения персонала в организации Аддиктивное поведение. Антисоциальное девиантное поведение. Суицидное поведение. Конформистское поведение. Нарцисстическое поведение. Эгоистическое, индивидуально-целевое деструктивное поведение. Фанатическое поведение. Аутистическое поведение Тема 3. Кадровая безопасность организации: понятия и сущность. Управление персоналом. Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ. Аналитическая деятельность по изучению персонала.

	Организация собеседования. Сведения, которые важно знать о кандидате. Проведение дознания. Сопровождающие проверки. Тестирование **Раздел 2. Управление корпоративной безопасностью в организации** Тема 4. Структура управления кадровой безопасности организации Принципы управления кадровой безопасности организации: целостности, срочности, надежности, правомерности, экономичности, согласованности, открытости и приватности, профессионализма Тема 5. Субъекты и объекты системы управления корпоративной безопасностью в организации Причины угроз системы управления корпоративной безопасностью: политико-идеологические, социально-экономические, психологические, моральные, национальные, физиологические, стратегические, профессиональные, финансовые Тема 6. Условия эффективного функционирования системы управления корпоративной безопасностью в организации Системный подход. Определение приоритета мероприятий по предотвращению потенциальных угроз. Ориентированность системы на обеспечение приоритетной защиты конфиденциальной информации. Непосредственное участие должностных лиц в обеспечении безопасности организации. Обеспечение взаимодействия системы с другими направлениями деятельности. Соразмерность затрат уровню угроз. Формализованное закрепление полномочий (предела компетенции) службы безопасности. Тема 7. Обеспечение кадровой безопасности при найме и увольнении персонала Защита от криминальных структур. Проверка на склонность к к вредным привычкам. Защита секретов производства (ноу-хау), защита баз данных, результатов маркетинговых исследований, планов и другой информации, важной для сохранения конкурентоспособности. Соответствие работника требованиям организационной культуры. Тема 8. Развитие лояльности персонала для обеспечения корпоративной безопасности в организации Создание атмосферы честности, открытости и взаимопомощи. Ликвидация элементов кадровой политики, способствующих мошенничеству. Помощь сотрудникам е. Специальная подготовка менеджеров и сотрудников противостоянию мошенничеству. Проверка персонала. Правовое и юридическое обеспечение Тема 9. Контроль персонала как условие обеспечения корпоративной безопасности организации Основные направления обеспечения корпоративной безопасности организации: нормативное, организационное, профессиональное и финансовое). Формы контроля: предварительный, текущий и итоговый
Формы текущего контроля	тесты, контрольные работы, практические занятия
Форма промежуточной аттестации	Экзамен

4.3.1. Перечень семинарских, практических занятий и лабораторных работ

№ п/п	№ раздела и темы дисциплины (модуля)	Наименование семинаров, практических и лабораторных работ	Трудоемкость (час.)		Оценочные средства	Формируемые компетенции
			Всего часов	Из них практическая подготовка		
1	Раздел 1.	Основы корпоративной безопасности	6		УО	ПК-3
2	Раздел 2.	Управление корпоративной безопасностью в организации	10			

4.3.2. Перечень тем (вопросов), выносимых на самостоятельное изучение самостоятельной работы студентов

№ п/п	Тема	Задание	Формируемая компетенция	ИДК
1	Аналитическая деятельность по изучению персонала	тестированию, подготовка отчета о практической работе	ПК-3	ПК-3.1

4.4. Методические указания по организации самостоятельной работы студентов

Самостоятельная работа студентов всех форм и видов обучения является одним из обязательных видов образовательной деятельности, обеспечивающей реализацию требований Федеральных государственных стандартов высшего профессионального образования. Согласно требованиям нормативных документов самостоятельная работа студентов является обязательным компонентом образовательного процесса, так как она обеспечивает закрепление получаемых на лекционных занятиях знаний путем приобретения навыков осмысления и расширения их содержания, навыков решения актуальных проблем формирования общекультурных и профессиональных компетенций, научно-исследовательской деятельности, подготовки к семинарам, лабораторным работам, сдаче зачетов и экзаменов. Самостоятельная работа студентов представляет собой совокупность аудиторных и внеаудиторных занятий и работ. Самостоятельная работа в рамках образовательного процесса в вузе решает следующие задачи:

— закрепление и расширение знаний, умений, полученных студентами во время аудиторных и внеаудиторных занятий, превращение их в стереотипы умственной и физической деятельности;

— приобретение дополнительных знаний и навыков по дисциплинам учебного плана;

— формирование и развитие знаний и навыков, связанных с научно-исследовательской деятельностью;

— развитие ориентации и установки на качественное освоение образовательной программы;

— развитие навыков самоорганизации;

— формирование самостоятельности мышления, способности к саморазвитию, самосовершенствованию и самореализации;

— выработка навыков эффективной самостоятельной профессиональной теоретической, практической и учебно-исследовательской деятельности.

Подготовка к практическому занятию. Подготовка к практическому занятию включает следующие элементы самостоятельной деятельности: четкое представление цели и задач его проведения; выделение навыков умственной, аналитической, научной деятельности, которые станут результатом предстоящей работы. Выработка навыков осуществляется с помощью получения новой информации об изучаемых процессах и с помощью знания о том, в какой степени в данное время студент владеет методами исследовательской деятельности, которыми он станет пользоваться на практическом занятии. Подготовка к практическому занятию нередко требует подбора материала, данных и специальных источников, с которыми предстоит учебная работа. Студенты должны дома подготовить к занятию 3–4 примера формулировки темы исследования, представленного в монографиях, научных статьях, отчетах. Затем они самостоятельно осуществляют поиск соответствующих источников, определяют актуальность конкретного исследования процессов и явлений, выделяют основные способы

доказательства авторами научных работ ценности того, чем они занимаются. В ходе самого практического занятия студенты сначала представляют найденные ими варианты формулировки актуальности исследования, обсуждают их и обосновывают свое мнение о наилучшем варианте. Время на подготовку к практическому занятию по нормативам составляет не менее 0,2 часа.

Подготовка к семинарскому занятию. Самостоятельная подготовка к семинару направлена: на развитие способности к чтению научной и иной литературы; на поиск дополнительной информации, позволяющей глубже разобраться в некоторых вопросах; на выделение при работе с разными источниками необходимой информации, которая требуется для полного ответа на вопросы плана семинарского занятия; на выработку умения правильно выписывать высказывания авторов из имеющихся источников информации, оформлять их по библиографическим нормам; на развитие умения осуществлять анализ выбранных источников информации; на подготовку собственного выступления по обсуждаемым вопросам; на формирование навыка оперативного реагирования на разные мнения, которые могут возникать при обсуждении тех или иных научных проблем. Время на подготовку к семинару по нормативам составляет не менее 0,2 часа.

Подготовка к контрольной работе. Контрольная работа назначается после изучения определенного раздела (разделов) дисциплины и представляет собой совокупность развернутых письменных ответов студентов на вопросы, которые они заранее получают от преподавателя. Самостоятельная подготовка к контрольной работе включает в себя: — изучение конспектов лекций, раскрывающих материал, знание которого проверяется контрольной работой; повторение учебного материала, полученного при подготовке к семинарским, практическим занятиям и во время их проведения; изучение дополнительной литературы, в которой конкретизируется содержание проверяемых знаний; составление в мысленной форме ответов на поставленные в контрольной работе вопросы; формирование психологической установки на успешное выполнение всех заданий. Время на подготовку к контрольной работе по нормативам составляет 2 часа.

Подготовка к экзамену. Самостоятельная подготовка к экзамену схожа с подготовкой к зачету, особенно если он дифференцированный. Но объем учебного материала, который нужно восстановить в памяти к экзамену, вновь осмыслить и понять, значительно больше, поэтому требуется больше времени и умственных усилий. Важно сформировать целостное представление о содержании ответа на каждый вопрос, что предполагает знание разных научных трактовок сущности того или иного явления, процесса, умение раскрывать факторы, определяющие их противоречивость, знание имен ученых, изучавших обсуждаемую проблему. Необходимо также привести информацию о материалах эмпирических исследований, что указывает на всестороннюю подготовку студента к экзамену. Время на подготовку к экзамену по нормативам составляет 36 часов для бакалавров.

Формы внеаудиторной самостоятельной работы

Составление глоссария Цель самостоятельной работы: повысить уровень информационный культуры; приобрести новые знания; отработать необходимые навыки в предметной области учебного курса. Глоссарий — словарь специализированных терминов и их определений. Статья глоссария — определение термина. Содержание задания: сбор и систематизация понятий или терминов, объединенных общей специфической тематикой, по одному либо нескольким источникам. Выполнение задания: 1) внимательно прочитать работу; 2) определить наиболее часто встречающиеся термины; 3) составить список терминов, объединенных общей тематикой; 4) расположить термины в алфавитном порядке; 5) составить статьи глоссария: — дать точную формулировку термина в именительном падеже; — объемно раскрыть смысл данного термина Планируемые результаты самостоятельной работы: способность студентов решать стандартные задачи

профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

Разработка проекта (индивидуального, группового) Цель самостоятельной работы: развитие способности прогнозировать, проектировать, моделировать. Проект — «ограниченное во времени целенаправленное изменение отдельной системы с установленными требованиями к качеству результатов, возможными рамками расхода средств и ресурсов и специфической организацией». Выполнение задания: 1) диагностика ситуации (проблематизация, целеполагание, конкретизация цели, форматирование проекта); 2) проектирование (уточнение цели, функций, задач и плана работы; теоретическое моделирование методов и средств решения задач; детальная проработка этапов решения конкретных задач; пошаговое выполнение запланированных проектных действий; систематизация и обобщение полученных результатов, конструирование предполагаемого результата, пошаговое выполнение проектных действий); 3) рефлексия (выяснение соответствия полученного результата замыслу; определение качества полученного продукта; перспективы его развития и использования). Предполагаемые результаты самостоятельной работы: готовность студентов использовать знание современных проблем науки и образования при решении образовательных и профессиональных задач; готовность использовать индивидуальные креативные способности для оригинального решения исследовательских задач; — способность прогнозировать, проектировать, моделировать.

Выполнение кейс-задания Цель самостоятельной работы: формирование умения анализировать в короткие сроки большой объем неупорядоченной информации, принятие решений в условиях недостаточной информации. Кейс-задание (англ. case — случай, ситуация) — метод обучения, основанный на разборе практических проблемных ситуаций — кейсов, связанных с конкретным событием или последовательностью событий. Виды кейсов: иллюстративные, аналитические, связанные с принятием решений. Выполнение задания: 1) подготовить основной текст с вопросами для обсуждения: — титульный лист с кратким запоминающимся названием кейса; — введение, где упоминается герой (герои) кейса, рассказывается об истории вопроса, указывается время начала действия; — основная часть, где содержится главный массив информации, внутренняя интрига, проблема; — заключение (в нем решение проблемы, рассматриваемой в кейсе, иногда может быть не завершено); 2) подобрать приложения с подборкой различной информации, передающей общий контекст кейса (документы, публикации, фото, видео и др.); 3) предложить возможное решение проблемы. Планируемые результаты самостоятельной работы: — способность студентов анализировать результаты научных исследований и применять их при решении конкретных исследовательских задач; — готовность использовать индивидуальные креативные способности для оригинального решения исследовательских задач; — способность решать нестандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий.

Составление тематического портфолио работ Цель самостоятельной работы: развитие способности к систематизации и анализу информации по выбранной теме, работе с эмпирическими данными, со способами и технологиями решения проблем. Тематическое портфолио работ — материалы, отражающие цели, процесс и результат решения какой-либо конкретной проблемы в рамках той или иной темы курса (модуля). Портфолио работ состоит из нескольких разделов (согласуются с преподавателем). Структура тематического портфолио работ: — сопроводительный текст автора портфолио с описанием цели, предназначения и краткого описания документа; — содержание или оглавление; органайзер (схемы, рисунки, таблицы, графики, диаграммы, гистограммы); лист наблюдений за процессами, которые произошли за время работы; письменные работы; видеофрагменты, компьютерные программы; рефлексивный журнал (личные

соображения и вопросы студента, которые позволяют обнаружить связь между полученными и получаемыми знаниями). Выполнение задания: 1) обосновать выбор темы портфолио и дать название своей работе; 2) выбрать рубрики и дать им названия; 3) найти соответствующий материал и систематизировать его, представив в виде конспекта, схемы, кластера, интеллект-карты, таблицы; 4) составить словарь терминов и понятий на основе справочной литературы; 5) подобрать необходимые источники информации (в том числе интернет-ресурсы) по теме и написать тезисы; 6) подобрать статистический материал, представив его в графическом виде; сделать выводы; 7) подобрать иллюстративный материал (рисунки, фото, видео); 8) составить план исследования; 27 9) провести исследование, обработать результаты; 10) проверить наличие ссылок на источники информации. Планируемые результаты самостоятельной работы: — готовность студентов использовать индивидуальные креативные способности для оригинального решения исследовательских задач; — повышение информационной культуры студентов и обеспечение их готовности к интеграции в современное информационное пространство; — способность использовать современные способы и технологии решения проблем.

Информационный поиск Цель самостоятельной работы: развитие способности к проектированию и преобразованию учебных действий на основе различных видов информационного поиска. Информационный поиск — поиск неструктурированной документальной информации. Список современных задач информационного поиска: решение вопросов моделирования; классификация документов; фильтрация, классификация документов; проектирование архитектур поисковых систем и пользовательских интерфейсов; извлечение информации (аннотирование и реферирование документов); выбор информационно-поискового языка запроса в поисковых системах. Содержание задания по видам поиска: поиск библиографический — поиск необходимых сведений об источнике и установление его наличия в системе других источников. Ведется путем разыскания библиографической информации и библиографических пособий (информационных изданий); поиск самих информационных источников (документов и изданий), в которых есть или может содержаться нужная информация; — поиск фактических сведений, содержащихся в литературе, книге (например, об исторических фактах и событиях, о биографических данных из жизни и деятельности писателя, ученого и т. п.). Выполнение задания: 1) определение области знаний; 2) выбор типа и источников данных; 3) сбор материалов, необходимых для наполнения информационной модели; 4) отбор наиболее полезной информации; 5) выбор метода обработки информации (классификация, кластеризация, регрессионный анализ и т.д.); 6) выбор алгоритма поиска закономерностей; 7) поиск закономерностей, формальных правил и структурных связей в собранной информации; 8) творческая интерпретация полученных результатов. Планируемые результаты самостоятельной работы: — способность студентов решать стандартные задачи профессиональной деятельности на основе информационной ибиблиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; готовность использовать знание современных проблем науки и образования при решении образовательных и профессиональных задач.

В ФБГОУ ВО «ИГУ» организация самостоятельной работы студентов регламентируется Положением осамостоятельной работе студентов, принятым Ученым советом ИГУ 22 июня 2012 г.

4.5. Примерная тематика курсовых работ (проектов)

По данной дисциплине выполнение курсовых проектов (работ) не предусматривается.

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

а) основная литература

1. Краковский, Юрий Мечеславович. Информационная безопасность и защита информации :учеб.пособие / Ю. М. Краковский. - Ростов н/Д :МарТ, 2008. - 287 с. ; 21 см. - (Учебный курс). - ISBN 978-5-241-00925-8 - :38 экз.11

2. Мельников, Владимир Павлович. Информационная безопасность и защита информации :учеб.пособие / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; ред. С. А. Клейменов. - 4-е изд., стер. - М. : Академия, 2009. - 331 с. ; 21 см. - (Высшее профессиональное образование : информатика и вычислительная техника). - ISBN 978-5-7695-6150-4 49 экз.

3. Нестеров, Сергей Александрович. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ [Электронный ресурс] : учебник и практикум / Нестеров С.А. - М. : Издательство Юрайт, 2016. - 321 с. - (Университеты России). - Режим доступа: http://www.biblioonline.ru/book/44CE6B76-7554-4E65-BC10-D7F267D88DD0. - Режим доступа: "ЭБС Юрайт". - неогранич. доступ. - ISBN 978-5-9916-7227-6

4. Нестеров, С. А. Основы информационной безопасности [Электронный ресурс] / С. А. Нестеров. - Москва : Лань, 2017. - Режим доступа: https://e.lanbook.com/book/90153. - Режим доступа: ЭБС "Издательство Лань". - Неогранич. доступ. - ISBN 978-5-8114-2290-6

б) дополнительная литература

1. Акулов, Олег Анатольевич. Информатика : базовый курс: учебник / О. А. Акулов, Н. В. Медведев. - 6-е изд., испр. и доп. - М. : Омега-Л, 2009. - 574 с. : ил. ; 21 см. - (Высшее техническое образование). - ISBN 978-5-370-01022-4: 39 экз.

2. Гринберг, А. С. Информационные технологии управления [Электронный ресурс] :учеб.пособие / А. С. Гринберг, Н. Н. Горбачев, А. С. Бондаренко. - Электрон. Текстовые дан. - Москва : ЮНИТИ-ДАНА, 2015. - 479 с. ; есть. - Режим доступа: http://rucont.ru/efd/352856?urlId=ArrmvDnhe1OJXKo7OIEeK5uspqMnOM29fKeOiwRo0pfndTiRqEuzQM7vjM5ERjnrPWMIXOZ0fapCp7WJYLILrw==. - Режим доступа: ЭБС "РУКОНТ". - Неогранич. доступ. - ISBN 978-5-238-00725-6 :

3. Орлов, С. А. Организация ЭВМ и систем [Электронный ресурс] : учебник для вузов. 3-е изд. / А. Орлов. - Санкт-Петербург :Питер, 2014. - 688 с. - Режим доступа: http://ibooks.ru/reading.php?productid=340894 http://ibooks.ru/product.php?productid=340894). - Режим доступа: ЭБС "Айбукс". - Неогранич. доступ. - Стандарт третьего поколения. - ISBN 978-5-496-01145-7 :

4. Платонов, Владимир Владимирович. Программно-аппаратные средства защиты информации [Электронный ресурс] :учеб.для студ. вузов, обуч. по напр. подгот. "Информ. безопасность" / В. В. Платонов. - ЭВК. - М. : Академия, 2013. - Режим доступа: . - Режим доступа: ЭЧЗ "Библиотех". - 20 доступ. - ISBN 978-5-7695-9327-7 :

в) список авторских методических разработок

1. Фрязинов А.В. Практикум по дисциплине «Защита персональных данных, автоматизация управленческой деятельности». – Иркутск, ИГУ, 2018. – 68 с.

г) базы данных, информационно-справочные и поисковые системы

1. Открытая электронная база ресурсов и исследований «Университетская информационная система РОССИЯ» [Электронный ресурс] : сайт. – Режим доступа: http://uisrussia.msu.ru бессрочный

2. Государственная информационная система «Национальная электронная библиотека» [Электронный ресурс] : сайт. – Режим доступа: http://нэб.рф. бессрочный

3. Научная электронная библиотека «ELIBRARY.RU» [Электронный ресурс] : сайт. – Режим доступа: http://elibrary.ru/defaultx.asp. - Контракт № 148 от 23.12.2020 г. Акт от 24.12.2020 г. срок действия по 31.12. 2021 г. доступ: http://elibrary.ru/

4. 4. ЭБС «Издательство Лань». Контракт № 100 от 13.11.2020 г. Акт № 671 от 14.11.2020 г.; Срок действия по 13.11.2021 г. доступ: www.e.lanbook.com, Контракт № 100 от 13.11.2020 г. Акт № Э 656 от 14.11.2020 г. ; Срок действия по 13.11.2021 г. доступ: www.e.lanbook.com

5. ЭБС ЭЧЗ «Библиотех». Государственный контракт № 019 от 22.02.2011 г. ООО «Библиотех». Лицензионное соглашение к Государственному контракту № 019 от 22.02.2011. Адрес доступа: https://isu.bibliotech.ru/ Срок действия: бессрочный.

6. ЭБС «Руконт» Контракт № 98 от 13.11.2020 г.; Акт № бК-5415 от 14.11.20 г. Срок действия по 13.11.2021г. доступ: http://rucont.ru/

7. ЭБС «Айбукс.ру/ibooks.ru» Контракт № 99 от 13.11.2020г.; Акт № 99А от 13.11.2020 г. Срок действия по 13.11.2021 г. доступа: http://ibooks.ru

8. ООО «Электронное издательство Юрайт». Контракт № 60 от 23.09.2020г. Акт приема-передачи № 3263 от 18.10.2020; Срок действия по 17.10. 2021 г. доступ: https://urait.ru/

9. Лицензионный контракт № 04-Е-0258 от 20.09.2021г. Акт приема-передачи № 5684 от 18.10.2021; Срок действия по 17.10. 2022 г. доступ: https://urait.ru/

10. ООО «ИВИС», контракт № 157 от 25. 12.2020 г.; Акт от 25.12.2020 г. Срок действия с 01.01.2021 по 31.12.2021 г. доступ: http://dlib.eastview.com

11. ООО «ИД «Гребенников», контракт № 147 от 23. 11.2020 г.; Акт от 25.12.2020 г. Срок действия с 01.01.2021 по 31.12.2021 г. доступ: http://grebennikon.ru

VI. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Учебно-лабораторное оборудование:

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
Специальные помещения: Учебная аудитория для проведения занятий лекционного и семинарского типа, текущего контроля, промежуточной аттестации.	Аудитория оборудована специализированной учебной мебелью, техническими средствами обучения, служащими для представления информации большой аудитории: Ноутбук(AserAspirev3-5516 (AMDA10-4600M 2300 Мгц)) (1 штука) с неограниченным доступом к сети Интернет, с неограниченным доступом к сети Интернет; Проектор Vivitek, экран ScreenVtdiaEcot- 3200*200MW 1:1, колонки ,наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации, соответствующие рабочей программе дисциплины Учебная лаборатория: компьютеры для проведения практических работ (Системный блок AMDAthlon-64 X3 445 3100 МГц), Монитор LG F1742S	ОС Windows: DreamSpark Premium, Договор № 03-016-14 от 30.10.2014 Microsoft Office: 0365ProPiusOpenStudents ShrdSvr ALNG subs VL NL I MthAcdmsStdnt w/Faculty (15000 лицензий) Kaspersky Endpoint Security длябизнеса- стандартный Russian Edition. 1500-2499 Node 1 year Educational License № 1B08170221054045-730177 BusinessStudio Лицензия № 7464 (бессрочно)

	(2 штуки), Монитор ViewSonic VA703b(24 штуки) с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации; проектор Sony XGA VPLSX535, экран ScreenVtdiaEcot-3200*200MW 1:1	
Специальные помещения: компьютерный класс (учебная аудитория) для групповых и индивидуальных консультаций, курсового проектирования (выполнениякурсовых работ), организации самостоятельной работы, в том числе, научно-исследовательской	Аудитория оборудована специализированной учебной мебелью, техническими средствами обучения: компьютеры (системный блок AMD Athlon 64 X2 DualCore 3600+ 1900 МГц (15 штук), Монитор LGFlatron L1742SE (14 штук), Монитор ViewSonic VG720) с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.	ОС Windows: DreamSpark Premium, Договор № 03-016-14 от 30.10.2014 Microsoft Office: 0365ProPiusOpenStudents ShrdSvr ALNG subs VL NL I MthAcdmsStdnt w/Faculty (15000 лицензий Kaspersky Endpoint Security длябизнеса- стандартный Russian Edition. 1500-2499 Node 1 year Educational License № 1B08170221054045-730177

6.2. Программное обеспечение:

№	Наименование Программного продукта	Кол-во	Обоснование для пользования ПО	Дата выдачи лицензии	Срок действия права пользования
1.	BusinessStudio 4.0	50	Лицензия № 7464	2015	бессрочно
2.	Directum 5.1	30	Лицензия № 26057	2016	1год
3.	Microsoft Office Professional Plus 2007 Russian Academic OPEN No Level	25	Номер Лицензии Microsoft 46211164 Гос.контракт № 03-162-09 от 01.12.2009	01.12.2009	бессрочно
4.	Microsoft Office Professional Plus 2007 Russian Academic OPEN No Level	10	Номер Лицензии Microsoft 42095516	27.04.2007	бессрочно
5.	Microsoft SQL Server 2012	1	Номер Лицензии Microsoft 65343111		бессрочно
6.	Microsoft Windows Server 2008 r2 Enterprise	1	Номер Лицензии Microsoft 49413875		бессрочно
7.	Microsoft® Windows® Professional 7 Russian Upgrade Academic OPEN No Level Promo	12	Номер Лицензии Microsoft 46211164 Гос.контракт № 03-162-09 от 01.12.2009	01.12.2009	бессрочно
8.	Microsoft®WinSL 8.1 Russian Academic OLP 1License NoLevel Legalization GetGenuine	130	Microsoft Invoice Number: 9564547610 ООО 'ИЦ 'Сиброн'	22.12.2014	бессрочно
9.	OpenOffice 4.1.3	Условия правообладателя	Условия использования по ссылке: https://www.openoffice.org/licenses/PDL.html	Условия правообладателя	бессрочно

6.3. Технические и электронные средства:

Методической концепцией преподавания предусмотрено использование технических и электронных средств обучения и контроля знаний студентов: мультимедийные презентации, фрагменты фильмов.

VII. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

При реализации программы данной дисциплины используются различные образовательные технологии.

При реализации программы данной дисциплины используются различные образовательные технологии.

1.	Разноуровневое обучение	У преподавателя появляется возможность помогать слабому, уделять внимание сильному, реализуется желание сильных учащихся быстрее и глубже продвигаться в образовании. Сильные учащиеся утверждаются в своих способностях, слабые получают возможность испытывать учебный успех, повышается уровень мотивации ученья.
2.	Лекционно-семинарскозачетная система	Данная система дает возможность сконцентрировать материал в блоки и преподносить его как единое целое, а контроль проводить по предварительной подготовке обучающихся
3.	Информационно-коммуникационные технологии	Изменение и неограниченное обогащение содержания образования, использование интегрированных курсов, доступ в ИНТЕРНЕТ.
4.	Систему инновационной оценки «портфолио»	Формирование персонифицированного учета достижений обучающегося как инструмента педагогической поддержки социального самоопределения, определения траектории индивидуального развития личности

Наименование тем занятий с использованием активных форм обучения:

№	Тема занятия	Вид занятия	Форма / Методы интерактивного обучения	Кол-во часов
1	Состав и содержание мер по обеспечению корпоративной безопасности персональных данных	ПЗ	Разработка проекта	4
Итого часов				4

VIII. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.1. Оценочные средства текущего контроля

№ п\п	Вид контроля	Контролируемые темы (разделы)	Компетенции, компоненты которых контролируются
1.		Раздел 1. Основы корпоративной безопасности	ПК-3
2.	УО, тестирование	Раздел 2. Управление корпоративной безопасностью в организации	

Применяется фонд контрольных практических заданий, тестов.

Оценочные средства предоставляются студентам в информационно-образовательной среде FORLABS (http://forlabs.ru).

Примеры тестов для текущего контроля

Задание #1

Вопрос:

Что относится к ***нижнему уровню*** политики безопасности?

Выберите несколько из 3 вариантов ответа:

1) требования к конкретным информационным сервисам

2) обеспечение базы для соблюдения законов и правил

3) спецификах отдельных видов услуг

Задание #2

Вопрос:

Какие из утверждений, относящиеся к ***управлению рисками***, являются верными?

Выберите несколько из 3 вариантов ответа:

1) Суть мероприятий по управлению рисками состоит в том, чтобы закупить и настроить необходимое защитное оборудование и программные средства

2) Когда возможный ущерб неприемлемо велик, необходимо принять экономически оправданные меры защиты

3) Периодическая (пере) оценка рисков необходима для контроля эффективности деятельности в области безопасности и для учета изменений обстановки

Задание #3

Вопрос:

Какие из утверждений, относящиеся к ***управлению рисками***, являются верными?

Выберите несколько из 3 вариантов ответа:

1) Оценивая размер ущерба, необходимо иметь в виду только непосредственные расходы на замену оборудования или восстановление информации

2) Рассматриваемые виды угроз следует выбирать исходя из соображений здравого смысла

3) Целесообразно выявлять не только сами угрозы, но и источники их возникновения

Задание #4

Вопрос:

К ***административному уровню*** информационной безопасности относятся...

Выберите один из 3 вариантов ответа:

1) действия общего характера, предпринимаемые руководством организации

2) меры безопасности, которые ориентированы на людей, а не на технические средства

3) меры, направленные на создание и поддержание в обществе негативного (в том числе с применением наказаний) отношения к нарушениям и нарушителям информационной безопасности

Задание #5

Вопрос:

Политика безопасности - это...

Выберите один из 3 вариантов ответа:

1) специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении лицензионных требований и условий, выданное лицензирующим органом юридическому лицу или индивидуальному предпринимателю

2) совокупность документированных решений, принимаемых руководством организации и направленных на защиту информации и ассоциированных с ней ресурсов

3) документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям

Задание #6

Вопрос:

Политика безопасности строится на основе...

Выберите один из 3 вариантов ответа:

1) определении обязанностей в соответствии с должностными инструкциями

2) анализа рисков

3) выделении пользователям только тех прав доступа, которые необходимы им для выполнения служебных обязанностей

Задание #7

Вопрос:

Управление рисками включает в себя следующие виды деятельности, которые чередуются циклически:

Выберите несколько из 3 вариантов ответа:

1) закупку и настройку программного обеспечения, обеспечивающего защиту

2) (пере)оценка (измерение) рисков

3) выбор эффективных и экономичных защитных средств

Задание #8

Вопрос:

Сопоставьте возможные действия по отношению к выявленным рискам

Укажите соответствие для всех 3 вариантов ответа:

1) заключение страхового соглашения

2) устранение причины риска

3) использование дополнительных защитных средств

__ уменьшение риска

__ переадресация риска

__ ликвидация риска

Задание #9

Вопрос:

В число ***аппаратных активов*** следует включить:

Выберите один из 3 вариантов ответа:

1) компьютеры, периферийные устройства, внешние интерфейсы, кабельное хозяйство, активное сетевое оборудование

2) данные, которые хранятся, обрабатываются и передаются по сети

3) прикладное программное обеспечение, инструментальные средства, средства управления сетью

Задание #10

Вопрос:

При формулировке целей политики нижнего уровня можно исходить из соображений...

Выберите несколько из 3 вариантов ответа:
1) целостности
2) неотказуемости
3) доступности

8.2. Оценочные средства для промежуточной аттестации

Тестовые задания (пример)

1. Что меньше всего поможет защите от компьютерных вирусов
□ Архивирование
□ Хранение файлов на неперезаписываемых оптических дисках
□ Проверка всех подключаемых носителей информации на выделенном компьютере
□ Установка программы – фильтра, контролирующей поступающие из сети файлы
□ Программы полифаги

2. Что не может являться источником компьютерных вирусов?
□ Всемирно известная сеть Internet
□ Программы, написанные хакерами
□ Устройства пиратской перезаписи
□ Программы фирмы Касперского

3. Какие способы не помогут защите информации в телекоммуникационных каналах
□ Метод защиты кодов паролей, хранимых в вычислительной системе
□ Процедура подтверждения характеристик данных
□ Управление маршрутом
□ Процедуры аутентификации
□ Цифровая подпись передаваемых сообщений

4. Зачем на смарт-картах с магнитной полосой выполняется рельефная печать
□ Чтобы слепые имели возможность использовать карты без посторонней помощи.
□ Подделка таких карт значительно осуществляется труднее
□ Чтобы банкомат считывал номер карты и фамилию владельца
□ Выполнение продумано дизайнерским решением
□ Чтобы карта могла читаться на ручных обрабатывающих машинах

5. Какой ответ не подходит к карте оптической памяти?
□ Карты оптической памяти имеют большую емкость, чем карта памяти.
□ Карты оптической памяти защищены от подделок лучше, чем магнитные карты
□ Данные на карты могут быть записаны только один раз.
□ Лазер прожигает в ячейках значение равное 0 или 1.
□ Карта может хранить до 16 Мбайт информации, например медицинские записи

6. Чего не бывает на пластиковой карте:

□ Имени владельца
□ Идентифицирующего кода
□ Имени изготовителя карты и его фирменный знак
□ Магнитной полосы на обратной стороне карты
□ Подписи владельца карты

7. На машинных носителях хранятся: (найти 1 неверный ответ)

□ информационные массивы общего информационного поля;
□ программные блоки, файлы, тома.
□ ведомость регистрации запросов должностных лиц на получение справок из ЭВМ
□ архивные данные;

8. Что не входит в систему контроля вскрытия аппаратуры?

□ Обеспечение определения места возникновения сигнала с точностью до технического средства;
□ Обеспечение отключения тревожной сигнализации по каждому техническому средству;
□ Обеспечение уменьшения уровня излучения технического средства, выведенного в ремонт
□ Обнаружение и запоминание нескольких одновременно возникающих сигналов вскрытия;
□ Обеспечение минимальной возможности скрытого обхода нарушителем цепей контроля;

9. В описании работы какой системы охранной сигнализации вкралась ошибка?

□ Внешнее освещение не влияет на работу системы прерывания ИК-луча.
□ Телевизионный извещатель перемещения опрашивает до 20 раз в секунду изображения с телевизионных камер сравнивая их с предыдущим.
□ Недостатком радиолокационных систем является трудность обнаружения медленно движущихся объектов.
□ Пневматическая система следит за изменением потока воздуха в просверленном из комнаты отверстии.
□ Микроволновая система настраивается так, чтобы люди находились в рабочее время в «мертвых» зонах где излучения почти нет.

10. Какие датчики не используют в традиционные системы охраны?

□ Датчики на токопроводящих линиях встроенные в оконное остекление и дверные проемы.
□ Подземные сейсмические датчики – геофоны, реагирующие на подкоп.
□ Датчики звукового давления, сигнализирующих о проломах витрин, потолков, стен.
□ Ёмкостные датчики, реагирующие на приближение человека к охраняемым объектам.
□ Датчики, реагирующие на разбивание, вырезание стекла.

11. Какие варианты применения ультразвуковых систем не существуют?

□ Датчики реагируют на прерывание ультразвукового луча
□ Облучения ультразвуком конкретных предметов (письменный стол, шкаф)
□ Ультразвуковой "луч" направляется на вход или на определенную зону помещения таким образом, что нарушитель обязательно его пересечет.
□ Охрана того места, через которое вероятнее всего будет проникать взломщик (вход, вестибюль, лестничная клетка).

12.Какие оргмероприятияв процессе создания системы защиты информации не всегда эффективны?

- ☐ Принятие законов по законодательной защите информации
- ☐ Введение на необходимых участках проведения работ с режимом секретности;
- ☐ Разграничение задач по исполнителям и выпуску документации;
- ☐ Установление и распределение ответственных лиц за утечку информации;
- ☐ Присвоение грифа секретности материалам, документации и хранение их под охраной

13. Какую информацию можно не защищать?

- ☐ Ценную информацию
- ☐ Несущественную информацию
- ☐ Полезную информацию
- ☐ Жизненно важную информацию
- ☐ Незаменимую информацию

14. Возможные каналы несанкционированного доступа в вычислительной системе

- ☐ Внутренний монтаж аппаратуры;
- ☐ Линии связи между аппаратными средствами данной вычислительной системы;
- ☐ Побочное электромагнитное излучение информации с аппаратуры системы;
- ☐ Логические и сенсорные ошибки человека
- ☐ Побочные наводки информации на вспомогательных и посторонних коммуникациях;

15. Какая из указанных причин не является случайным воздействием при эксплуатации автоматизированной системы могут быть:

- ☐ Отказы и сбои аппаратуры.
- ☐ Изменение потока и содержания сообщения.
- ☐ Помехи на линиях связи от воздействий внешней среды.
- ☐ Ошибки человека как звена системы.
- ☐ Схемные и системотехнические ошибки разработчиков.

16. Какое из мероприятий не поможет при организации парольной защиты

- ☐ Длина пароля должна исключать возможность его раскрытия путем подбора.
- ☐ Пароль не должен легко запоминаться
- ☐ Пароли должны периодически меняться.
- ☐ Пароль не выдается при вводе на экран монитора.
- ☐ Запись пароля значительно повышает вероятность его компрометации

17. На этапе эксплуатации целостность и доступность информации в системе не обеспечивается:

- ☐ противодействием перегрузкам и «зависаниям» системы
- ☐ повышением отказоустойчивости КС (компьютерной системы)
- ☐ использованием строго определенного множества программ
- ☐ дублированием информации
- ☐ перемещением по локально-вычислительным сетям.

18. Какой из защитных механизмов не относится к аппаратно программным комплексам защиты

- ☐ идентификация и аутентификация пользователей
- ☐ разграничение доступа к файлам, каталогам, дискам
- ☐ контроль целостности программных средств и информации;

□ электронный жетон — генератор случайных идентификационных кодов.
□ криптографическое преобразование информации;

19. Обычно для осуществления несанкционированного доступа к информации пользователь применяет:

□ знания о компьютерной системе и умения работать с ней
□ сведения о системе защиты информации
□ многоуровневый режим выполнения команд
□ сбои, отказы технических и программных средств
□ ошибки, небрежность обслуживающего персонала и пользователей.

20. Информационным оружием нельзя назвать следующие средства

□ фальсификация информации в каналах государственного и военного управления
□ уничтожения, искажения или хищения информационных массивов
□ преодоления систем защиты
□ ограничения допуска законных пользователей;
□ дезорганизации работы технических средств, компьютерных систем.

21. Внутренними угрозами, не представляющими опасность для объектов обороны, являются:

□ нерешенность вопросов защиты интеллектуальной собственности предприятий оборонного комплекса
□ преднамеренные действия, а также ошибки персонала информационных систем специального назначения;
□ диверсионно-подрывная деятельность специальных служб иностранных государств
□ нерешенность вопросов социальной защиты военнослужащих и членов их семей
□ информационные ресурсы, содержащие сведения, отнесенные к государственной тайне

22.К основным задачам в сфере обеспечения и регулирования информационной безопасности РФ не относятся:

□ координация деятельности органов государственной власти по обеспечению информационной безопасности;
□ доктрина информационной безопасности Российской Федерации;
□ совершенствование и защита отечественной информационной инфраструктуры;
□ защита государственных информационных ресурсов,
□ пропаганда средствами массовой информации элементов национальных культур народов России

23. В ситуациях, чреватых неопределенным исходом, инфологемы не выполняют следующие функции

□ охранная;
□ скрывающая;
□ отвлекающая;
□ объективная
□ дезориентирующая (подменяющая ориентиры)

24. Такой приём в «азбуке пропаганды» неизвестен

☐ «приклеивание или навешивание ярлыков»
☐ «свои ребята» или «игра в простонародность»
☐ «запугивание» или «красная угроза»
☐ «перетасовка» или «подтасовка карт»
☐ «сияющие обобщения» или «блистательная неопределенность»

25. Хаотизация системы высшего управления этими путями не осуществляется:
☐ изменение приоритетов государственного целеполагания;
☐ депрофессионализация и недееспособность ее аппаратов;
☐ средствми нейтрализации тестовых программ;
☐ создание атмосферы полной бесконтрольности и личной безответственности ее членов;
☐ возможность любого произвола относительно любых граждан и структур государства.

26. Такой метод обеспечения безопасности процессов переработки информации не применяется
☐ Опознание
☐ Маскировка
☐ Регламентация
☐ Принуждение
☐ Побуждение

27. Такие механизмы безопасности не используются:
☐ цифровая (электронная) подпись;
☐ обеспечение аутентификации;
☐ арбитраж, или освидетельствование;
☐ контроль доступа;
☐ целесообразность засекречивания.

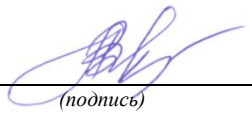
28. Таких рубежей для защиты с ценной конфиденциальной информацией не предусматривается:
☐ контролируемая территория;
☐ обслуживающий персонал;
☐ здание;
☐ устройство, носитель информации;
☐ информационные ресурсы.

29. Какой метод защиты от прослушивания акустических сигналов не применяется:
☐ звукоизоляция и звукопоглощение акустического сигнала;
☐ зашумление помещений или твердой среды для маскировки акустических сигналов;
☐ защита от несанкционированной записи речевой информации на диктофон;
☐ мониторинг трафика
☐ обнаружение и изъятие закладных устройств.

30. В защите и обработке информации в базах данных компьютерных систем этого метода нет
☐ Случайная последовательность сигналов помехи
☐ Блокировка ответа
☐ Коррекция данных и искажение ответа

- ☐ Разделение баз данных на группы
- ☐ Контроль поступающих ответов

Разработчики:

	профессор	Рохин А.В.
(подпись)	*(занимаемая должность)*	*(инициалы, фамилия)*

Документ составлен в соответствии с требованиями ФГОС ВО по направлению 09.03.03 «Прикладная информатика», утвержденного приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 г. № 922, с учетом требований профессиональных стандартов 06.013 «Специалист по информационным ресурсам», 06.015 «Специалист по информационным системам» и 06.024 «Специалист по технической поддержке информационно-коммуникационных систем»

Программа рассмотрена на заседании кафедры прикладной информатики и документоведения «04» марта 2022 г.

Протокол № 8. И.о.зав. кафедрой  А.В. Рохин

Настоящая программа, не может быть воспроизведена ни в какой форме без предварительного письменного разрешения кафедры-разработчика программы.