МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

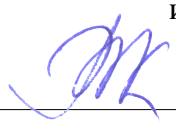
федеральное государственное бюджетное образовательное учреждение высшего образования

«ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ФГБОУ ВО «ИГУ»

Кафедра естественнонаучных дисциплин

УТВЕРЖДАЮ
Декан факультета бизнес-коммуникаций и информатики



_____ В.К. Карнаухова

«16» марта 2022 г

Рабочая программа дисциплины (модуля)

Наименование дисциплины (модуля) **Б1.О.22 Информационная безопасность**
(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 дизайне**

Квалификация выпускника: бакалавр

Форма обучения: очная
(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 естественнонаучных дисциплин:

Протокол № 7 от «11» марта 2022 г.

и.о. зав. кафедры  А.Г. Балахчи

Иркутск – 2022

СОДЕРЖАНИЕ

стр.

I. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ (МОДУЛЯ) 3
II. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО 3
III. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ 3
IV. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ 4
4.1 Содержание дисциплины, структурированное по темам, с указанием видов учебных занятий и СРС, отведенного на них количества академических часов 4
4.2 План внеаудиторной самостоятельной работы обучающихся по дисциплине 5
4.3 Содержание учебного материала 6
4.3.1. Перечень семинарских, практических занятий и лабораторных работ 7
4.3.2. Перечень тем (вопросов), выносимых на самостоятельное изучение самостоятельной работы студентов 7
4.4. Методические указания по организации самостоятельной работы студентов 8
4.5. Примерная тематика курсовых работ (проектов) 11
V. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ) 11
а) основная литература 11
б) дополнительная литература 11
в) периодическая литература 11
г) базы данных, информационно-справочные и поисковые системы 11
VI. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 12
6.1. Учебно-лабораторное оборудование 12
6.2. Программное обеспечение 14
6.3. Технические и электронные средства 14
VII. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ 14
VIII. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ 15
8.1. Оценочные средства текущего контроля 15
8.2. Оценочные средства для промежуточной аттестации 22

I. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ (МОДУЛЯ)

Цели: Сформировать у обучающихся комплекс теоретических знаний и практических навыков, достаточный для формирования важнейших представлений о теории и практике создания защищенных информационных систем, о проблемах информационной безопасности человека, общества, предприятия, о способах и средствах защиты информации в автоматизированных системах.

Задачи:

— Изучение направлений и нормативно-методических документов по защите информации;

— Изучение методов, форм и средств организационной защиты информации;

— Изучение технологии выполнения работ по защите информации;

— Изучение методов, форм и средств технической защиты информации;

— Изучение угроз информационной безопасности на объектах информатизации и применение специализированных аппаратных и программных средств по защите информации.

II. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

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

Дисциплина предназначена для закрепления знаний и умений в сфере проектирования, разработки, внедрения и эксплуатации информационных систем, управления их жизненным циклом и отработки практических навыков в области информационных и коммуникационных технологий.

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

— Дискретная математика;

— Информационные системы и технологии;

— Вычислительные системы и компьютерные сети;

— Управление проектами;

— Теория систем и системный анализ.

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

— Проектирование информационных систем;

— Стандартизация, сертификация и управление качеством программного обеспечения;

— Управление ИТ-сервисами и контентом.

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
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, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры 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 навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности
ОПК-4 Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	ОПК-4.1	Знает основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы
	ОПК-4.2	Умеет применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы
	ОПК-4.3	Владеет навыками составления технической документации на различных этапах жизненного цикла информационной системы

IV. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 4 зачетных единицы, 144 часа, в том числе 36 часов на контроль, из них 36 часов на экзамен.

Форма промежуточной аттестации: экзамен.

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

п/п	Раздел дисциплины/темы	Семестр	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		
1	Введение в безопасность информационных систем.	6	4	10	0	6	
2	Угрозы безопасности информационных систем и их реализация.	6	4	10	0	16	
3	Криптографические системы защиты информации.	6	4	10	0	16	
4	Программно-технические средства защиты информации.	6	4	4	0	20	
Итого за 6 семестр			**16**	**34**	**0**	**58**	**Экз (36)**
Итого часов			**16**	**34**	**0**	**58**	

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	Введение в безопасность информационных систем.	**Для овладения знаниями:** чтение учебной литературы, чтение дополнительной литературы, использование аудио- и видео-записей, компьютерной техники и интернета **Для закрепления и систематизации знаний:** работа с конспектом лекций, ответы на контрольные вопросы Подготовка к экзамену	1-4 учебная неделя	6	УО	Интернет, ЭБС, ЭИОС «Форлабс»

6	Угрозы безопасности информационных систем и их реализация.	**Для овладения знаниями:** чтение учебной литературы, чтение дополнительной литературы, использование аудио- и видео-записей, компьютерной техники и интернета **Для закрепления и систематизации знаний:** работа с конспектом лекций, ответы на контрольные вопросы Подготовка к экзамену	5-8 учебная неделя	16	УО	Интернет, ЭБС, ЭИОС «Форлабс»
6	Криптографические системы защиты информации.	**Для овладения знаниями:** чтение учебной литературы, чтение дополнительной литературы, использование аудио- и видео-записей, компьютерной техники и интернета **Для закрепления и систематизации знаний:** работа с конспектом лекций, ответы на контрольные вопросы **Для формирования умений:** решение задач Подготовка к экзамену	9-12 учебная неделя	16	Тест, УО	Интернет, ЭБС, ЭИОС «Форлабс»
6	Программно-технические средства защиты информации.	**Для овладения знаниями:** чтение учебной литературы, чтение дополнительной литературы, использование аудио- и видео-записей, компьютерной техники и интернета **Для закрепления и систематизации знаний:** работа с конспектом лекций, ответы на контрольные вопросы **Для формирования умений:** решение задач Подготовка к экзамену	13-16 учебная неделя	20	Тест, УО	Интернет, ЭБС, ЭИОС «Форлабс»
Общая трудоемкость самостоятельной работы по дисциплине (час)				**58**		
Из них объем самостоятельной работы с использованием электронного обучения и дистанционных образовательных технологий (час)				**0**		
Бюджет времени самостоятельной работы, предусмотренный учебным планом для данной дисциплины (час)				**58**		

4.3 Содержание учебного материала

Трудоемкость дисциплины (з.е.)	4
Наименование основных разделов (модулей)	Введение в безопасность информационных систем. Угрозы безопасности информационных систем и их реализация. Криптографические системы защиты информации. Программно-технические средства защиты информации.
Формы текущего контроля	Устный опрос, тест

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
1	1	Введение в безопасность информационных систем.	10	Тест, УО	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3
2	2	Угрозы безопасности информационных систем и их реализация.	10	Тест, УО	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3
3	3	Криптографические системы защиты информации. Система Диффи Хеллмана. Шифр Шамира. Шифр Эль-Гамаля. Шифр RSA. Электронная подпись.	10	Тест, УО, КР	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3
4	4	Программно-технические средства защиты информации.	4	Тест, УО	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3

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

№ п/п	Тема	Задание	Формируемая компетенция	ИДК
1	Введение в безопасность информационных систем.	Геополитическое информационное противоборство	ОПК-3, ОПК-4	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3

2	Угрозы безопасности информационных систем и их реализация.	Выявление атак и защита при когнитивном воздействии	ОПК-3, ОПК-4	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3
3	Криптографические системы защиты информации.	Потоковые методы шифрования.	ОПК-3, ОПК-4	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3
4	Программно-технические средства защиты информации.	Популярные средства защиты информации.	ОПК-3, ОПК-4	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3

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 лекции. Качество освоения содержания конкретной дисциплины прямо зависит от того, насколько студент сам, без внешнего принуждения формирует у себя установку на получение на лекциях новых знаний, дополняющих уже имеющиеся по данной дисциплине. Время на подготовку студентов к двухчасовой лекции по нормативам составляет не менее 0,2 часа.

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 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

Информационный поиск Цель самостоятельной работы: развитие способности к проектированию и преобразованию учебных действий на основе различных видов информационного поиска. Информационный поиск — поиск неструктурированной документ-

альной 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 и библиографической 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.

Разработка мультимедийной презентации Цели самостоятельной работы (варианты): — освоение (закрепление, обобщение, систематизация) учебного материала; — обеспечение контроля качества знаний; — формирование специальных компетенций, обеспечивающих возможность работы с информационными технологиями; — становление общекультурных компетенций. Мультимедийная презентация — представление содержания учебного материала, учебной задачи с использованием мультимедийных технологий.

Выполнение задания:

1. Этап проектирования: — определение целей использования презентации; — сбор необходимого материала (тексты, рисунки, схемы и др.); — формирование структуры и логики подачи материала; — создание папки, в которую помещен собранный материал.

2. Этап конструирования: — выбор программы MS PowerPoint в меню компьютера; — определение дизайна слайдов; — наполнение слайдов собранной текстовой и наглядной информацией; — включение эффектов анимации и музыкального сопровождения (при необходимости); — установка режима показа слайдов (титульный слайд, включающий наименование кафедры, где выполнена работа, название презентации, город и год; содержательный — список слайдов презентации, сгруппированных по темам сообщения; заключительный слайд содержит выводы, пожелания, список литературы и пр.).

3. Этап моделирования — проверка и коррекция подготовленного материала, определение продолжительности его демонстрации.

Планируемые результаты самостоятельной работы: — повышение информационной культуры студентов и обеспечение их готовности к интеграции в современное информационное пространство; — способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; — способность к критическому восприятию, обобщению, анализу профессиональной информации, постановке цели и выбору путей ее достижения; — способность применять современные методики и технологии организации и реализации образовательного процесса на различных образовательных ступенях в различных образовательных учреждениях; — готовность использовать индивидуальные креативные способности для оригинального решения исследовательских задач.

В ФБГОУ ВО «ИГУ» организация самостоятельной работы студентов регламентируется Положением о самостоятельной 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 Ю. М. Информационная безопасность и защита информации: учеб. пособие / - Ростов н/Дону: МарТ, 2008. - 287 с.

2. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ [Электронный ресурс] : учебник / Лось А.Б., Нестеренко А.Ю., Рожков М.И. - Москва. : Издательство Юрайт, 2016. - 473 с. - (Бакалавр. Академический курс). - Режим доступа: "ЭБС Юрайт". неогранич. доступ

3. Нестеров С. А. Основы информационной безопасности [Электронный ресурс] / - Москва: Лань, 2017. - Режим доступа: ЭБС "Издательство Лань". неогранич. доступ.

б) дополнительная литература

1. Введение в защиту информации в атоматизированных системах [Текст] : учеб. пособие для студ. / А. А. Малюк, С. В. Пазизин, Н. С. Погожин. - 4-е изд., стер. - Москва.: Горячая линия -Телеком, 2011. - 146 с. ; 20 см. - Библиогр.: с. 143-145. - ISBN 978-5-9912-0181-0

2. Нестеров С.А. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ [Электронный ресурс] : учебник и практикум / - Москва: Издательство Юрайт, 2016. - 321 с. - (Университеты России). - Режим доступа: "ЭБС Юрайт". - неогранич. доступ.

в) периодическая литература

Нет.

г) базы данных, информационно-справочные и поисковые системы

1. 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/

2. Открытая электронная база ресурсов и исследований «Университетская

информационная система РОССИЯ» [Электронный ресурс] : сайт. – Режим доступа: http://uisrussia.msu.ru бессрочный

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

В соответствии с п. 4.3.4. ФГОС ВО, обучающимся в течение всего периода обучения обеспечен неограниченный доступ (удаленный доступ) к электронно-библиотечным системам:

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

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

— Научная электронная библиотека «ELIBRARY.RU» [Электронный ресурс] : сайт. - Контракт № 148 от 23.12.2020 г. Акт от 24.12.2020 г. Срок действия по 31.12.2022 г. – Режим доступа: http://elibrary.ru/

— ЭБС «Издательство Лань». Контракт № 04-Е-0346 от 12.11.2021 г. № 976 от 14.11.2021 г. Срок действия по 13.11.2022 г. – Режим доступа: https://www.e.lanbook.com

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

— ЭБС «Руконт» ЦКБ «Бибком». № 04-Е-0343 от 12.11.2021 г. Акт № бК-5195 от 14.11.2021 г. Срок действия по 13.11.2022г. – Режим доступа: http://rucont.ru

— ЭБС «Айбукс.ру/ibooks.ru» ООО «Айбукс». Контракт № 04-Е-0344 от 12.11.2021 г.; Акт от 14.11.2021 г. Срок действия по 13.11.2022 г. – Режим доступа: http://ibooks.ru

— Электронно-библиотечная система «ЭБС Юрайт». ООО «Электронное издательство Юрайт». Контракт № 04-Е-0258 от 20.09.2021г. Контракт № 04-Е-0258 от 20.09.2021 г. Срок действия по 17.10. 2022 г. – Режим доступа: https://urait.ru

— УБД ИВИС. Контракт № 04-Е-0347 от 12.11.2021 г. Акт от 15.11.2021 г. Срок действия с 01.01.2022 по 31.12.2022 г. – Режим доступа: http://dlib.eastview.com

— Электронная библиотека ИД Гребенников. Контракт № 04-Е-0348 от 12.11.2021г.; Акт № 348 от 15.11.2021 г. Срок действия с 01.01.2022 по 31.12.2022 – Режим доступа: 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; Проектор Vivitek, экран ScreenVtdiaEcot- 3200*200MW 1:1, колонки, наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации, соответствующие рабочей программе дисциплины «Архитектурный подход к развитию предприятий и информационных систем». Учебная лаборатория: компьютеры для проведения практических работ (Системный блок AMDAthlon-64 X3 445 3100 МГц), Монитор LG F1742S (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	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. 15002499 Node 1 year Educational License № 1B08-170221-054045-730-177 BusinessStudio Лицензия № 7464 (бессрочно)

Специальные помещения: компьютерный класс (учебная аудитория) для групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых 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 для бизнеса- стандартный Russian Edition. 15002499 Node 1 year Educational License № 1B08¬170221-054045¬730¬177

6.2. Программное обеспечение

№	Наименование Программного продукта	Кол-во	Обоснование для пользования ПО	Дата выдачи лицензии	Срок действия права пользования
1	Microsoft Office: 0365ProPiusOpenStudents ShrdSvr ALNG subs VL NL I MthAcadmsStdnt w/Faculty	15000	Условия правообладателя	Условия правообладателя	Условия правообладателя

6.3. Технические и электронные средства

Методической системой 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.

Проблемное обучение	Создание в учебной деятельности проблемных ситуаций и организация активной самостоятельной деятельности учащихся по их разрешению, в результате чего происходит творческое овладение знаниями, умениями, навыками, развиваются мыслительные способности

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.
Проектные методы обучения	Работа по данной методике дает возможность развивать индивидуальные творческие способности учащихся, более осознанно подходить к профессиональному и социальному самоопределению
Исследовательские методы в обучении	Дает возможность учащимся самостоятельно пополнять свои знания, глубоко вникать в изучаемую проблему и предполагать пути ее решения, что важно при формировании мировоззрения. Это важно для определения индивидуальной траектории развития каждого обучающегося
Лекционно-семинарскозачетная система	Данная система дает возможность сконцентрировать материал в блоки и преподносить его как единое целое, а контроль проводить по предварительной подготовке обучающихся
Информационно-коммуникационные технологии	Изменение и неограниченное обогащение содержания образования, использование интегрированных курсов, доступ в ИНТЕРНЕТ.

Наименование тем занятий с использованием активных форм обучения:

№	Тема занятия	Вид занятия	Форма / Методы интерактивного обучения	Кол-во часов
1	Геополитическое информационное противоборство	практическое занятие	Круглый стол (дискуссия, дебаты)	2
2	Организация работ по ИБ в РФ	практическое занятие	Круглый стол (дискуссия, дебаты)	2
3	Методы информационного воздействия	практическое занятие	Круглый стол (дискуссия, дебаты)	2
4	Методы противодействия нарушению ИБ	практическое занятие	Круглый стол (дискуссия, дебаты)	2

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	Тест	Введение в безопасность информационных систем. Угрозы безопасности информационных систем и их реализация. Криптографические системы защиты информации. Программно-технические средства защиты информации.	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3
2	Устный опрос	Введение в безопасность информационных систем. Угрозы безопасности информационных систем и их реализация. Криптографические системы защиты информации. Программно-технические средства защиты информации.	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3
3	Контрольная работа	Криптографические системы защиты информации.	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3

Примеры оценочных средств для текущего контроля

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 сиг¬нала 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 оргмероприятия в 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 вычислитель¬ной 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 автоматизиро¬ванной 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 КС целостность и доступность инфор¬мации 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 ин¬формационных 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 без¬опасности 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

31. В комплекс защиты территории охраняемых объектов эта компонента не входит:

☐ система оповещения о попытках вторжения;

☐ оптическая (обычно телевизионная) система опознавания нарушителей;

☐ система аварийного предупреждения;

☐ оборонительная система (звуковая и световая сигнализация, применение в случае необходимости оружия);

☐ механическая система защиты.

8.2. Оценочные средства для промежуточной аттестации

Перечень примеров оценочных средств.

Вопросы:

— Классификация информационных ресурсов.

— Какие информационно-правовые ресурсы Вы знаете?

— Риски угроз информационным ресурсам.

— Что такое информационная безопасность?

— Основные направления информационной безопасности.

— Что понимается под угрозой безопасности информации?

— Принципы, методы и средства защиты информации.

— Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации в РФ.

— В чем заключается политика безопасности предприятия?

— Перечень защищаемой информации организации на примере туристического агентства.

— Дайте определение технического канала утечки информации.

— Какие технические каналы утечки информации Вы знаете?

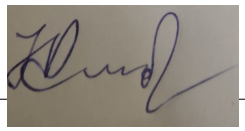
— Методы и средства защиты программ и данных в ЭВМ.

— Классификация вредоносных программ.
— Какие антивирусные программы Вы знаете?
— Какие защитные механизмы имеют современные операционные системы?
— Дайте определение несанкционированного доступа к информации.
— Методы и средств защиты информации от утечки по техническим каналам.
— Какие угрозы безопасности информации при вхождении в Интернет Вы знаете?
— Особенности защиты информации при вхождении в Интернет.
— Основные направления обеспечения конфиденциальности информации.
— Перечислите методы повышения достоверности информации в АС.
— Перечислите методы повышения сохранности информации в АС.
— Какие виды резервирования информации Вы знаете?
— Какие способы идентификации персонала Вы знаете?
— Перечислите основные функции системы разграничения доступа?
— Подходы к организации обучения персонала по вопросам защиты информации.
— Информационная безопасность и безопасность информации
— Необходимость обеспечения безопасности информационных систем
— Нормативно-правовые основы информационной безопасности
— Организационное обеспечение информационной безопасности
— Анализ формальных моделей безопасности
— Характеристика угроз безопасности информации
— Характеристика и классификация атак
— Виды и источники угроз информационной безопасности РФ
— Основные понятия криптографии
— Алгоритм DES и его развитие
— Российский алгоритм шифрования поколения
— Новый стандарт криптографической защиты США
— Двухключевые криптографические системы
— Сравнение симметричных и несимметричных алгоритмов шифрования
— Хэш-функция
— Цифровая подпись
— Общие принципы создания систем защиты информации
— Технические средства снятия информации
— Защита информации от побочных излучений
— Контроль целостности данных
— Руководящие документы Гостехкомиссии России

Примеры заданий:

нет

Разработчики:



	профессор	Н.В. Амбросов
	(занимаемая должность)	*(инициалы, фамилия)*

Программа составлена в соответствии с требованиями ФГОС ВО и учетом рекомендаций ПООП по направлению подготовки 09.03.03 «Прикладная информатика».

Программа рассмотрена на заседании кафедры естественнонаучных дисциплин

Протокол № 7 от «11» марта 2022 г.

и.о. зав. кафедры  А.Г. Балахчи

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