Автономная некоммерческая образовательная организация высшего образования
«Сибирский институт бизнеса и информационных технологий»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Информационная безопасность ИС»

(протокол решения Ученого совета № 4/Д от 11.01.2021 г.)

Направление подготовки
09.03.03 Прикладная информатика

Направленность
«Прикладная информатика в экономике»

Квалификация выпускника
«бакалавр»

Форма обучения (год набора)
очная (2021, 2022)
заочная (2021, 2022)

Омск – 2022

Рабочая программа дисциплины «Информационная безопасность ИС».

Автор(ы):
старший преподаватель  Е.В. Куликова

Рецензент(ы): А.Е. Ультан, доцент кафедры «Высшая математика и информатика» Омского филиала ФГОБУ ВО «Финансовый университет при Правительстве РФ», к.т.н.

Рабочая программа рассмотрена руководителем ОПОП:

 Е.В. Куликова

Рабочая программа одобрена Ученым советом института (протокол № 4/Д от 11 января 2021 г.)

(с изменениями и дополнениями от 01 сентября 2021 г., протокол решения УС № 1)

(с изменениями и дополнениями от 26.01.2022 г., протокол решения УС № 6)

Нормативно-правовую базу разработки рабочей программы дисциплины составляют:

- Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 09.03.03 Прикладная информатика (приказ Минобрнауки России от 19.09.2017 г. № 922)
- Приказ «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры» от 05 апреля 2017 г. № 301.
- Приказ «Об утверждении порядка перечней специальностей и направлений подготовки высшего образования» от 12 сентября 2013 г. № 1061.

- Основная профессиональная образовательная программа высшего образования направления подготовки бакалавриата 09.03.03 Прикладная информатика (направленность «Прикладная информатика в экономике»), утвержденная ректором 11.01.2021.
- Положение о комплектах оценочных материалов основной профессиональной образовательной программы высшего образования в АНОО ВО «Сибирский институт бизнеса и информационных технологий», утвержденное ректором 31.08.2020 г.

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОПОП БАКАЛАВРИАТА

Цель дисциплины «Информационная безопасность ИС» - - формирование фундаментальных знаний в области информационной безопасности информационных систем, подходов к анализу угроз информационной безопасности, освоение дисциплинарных компетенций для решения задач защиты информации в информационных системах;

- развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений.

Задачи дисциплины:

- изучение видов защищаемой информации, угроз информационной безопасности;
- изучение методов и средств обеспечения информационной безопасности информационных систем, механизмов защиты информации, формальных моделей безопасности, критериев оценки защищенности и обеспечения безопасности автоматизированных систем;
- приобретение умений в подборе программных, технических, организационных средств обеспечения информационной безопасности.

В результате освоения ОПОП бакалавриата обучающийся должен овладеть следующими результатами обучения по дисциплине:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Перечень планируемых результатов обучения по дисциплине
Общепрофессиональные компетенции (ОПК)		
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	**Знать:** 1. Основные угрозы безопасности информации и виды защищаемой информации 2. Основные требования и составляющие информационной безопасности 3. Стандарты в области информационной безопасности 4. Методы и средства обеспечения информационной безопасности компьютерных систем, механизмы защиты информации 5. Критерии оценки защищенности и обеспечения безопасности автоматизированных систем
	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	**Уметь:** 1. Анализировать виды угроз безопасности информации и информационных систем 2. Выбирать методы и средства обеспечения информационной безопасности компьютерных систем 3. Использовать программные, технические, организационные средства обеспечения информационной безопасности

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП БАКАЛАВРИАТА

Дисциплина «Информационная безопасность ИС» входит в обязательную часть учебного плана блока «Дисциплины, модули» основной профессиональной образовательной программы (Б1.О.24).

Данная дисциплина предусмотрена учебным планом в 7 семестре на очной форме и в 9 семестре на заочной форме обучения.

При изучении данного курса студенты опираются на знания и умения, полученные в результате освоения следующих дисциплин:

"Информатика и информационные технологии"

"Сети и системы передачи информации"

"Информационно-библиографическая культура"

Знания и умения, полученные в результате изучения данной дисциплины, используются в последующем для изучения:

"Выполнение и защита выпускной квалификационной работы"

3. ОБЪЕМ ДИСЦИПЛИНЫ В ЗАЧЕТНЫХ ЕДИНИЦАХ С УКАЗАНИЕМ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ, ВЫДЕЛЕННЫХ НА КОНТАКТНУЮ РАБОТУ ОБУЧАЮЩИХСЯ С ПРЕПОДАВАТЕЛЕМ (ПО ВИДАМ ЗАНЯТИЙ) И НА САМОСТОЯТЕЛЬНУЮ РАБОТУ ОБУЧАЮЩИХСЯ

Общая трудоемкость (объем) дисциплины составляет 3 з.е., 108 ч.

Вид учебной работы	Очная форма	Заочная форма
	7 семестр	9 семестр
Общая трудоемкость дисциплины	108	108
Контактная работа, в том числе в электронной информационно-образовательной среде (всего):	76	12
Лекционные занятия	36	4
Лабораторные занятия	18	2
Практические занятия	18	2
Консультации	4	4
Самостоятельная работа обучающихся (всего), в том числе:	23	92
Форма промежуточной аттестации обучающегося- зачет	9	4

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ, СТРУКТУРИРОВАННОЕ ПО ТЕМАМ (РАЗДЕЛАМ) С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ

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

7 семестр очная форма обучения

Раздел/тема дисциплины, содержание	Всего, час.	Объем часов (по видам учебных занятий)							Код индикатора достижения компетенции
		Всего, час.	Контактная работа (по учебным занятиям), час.				Самостоятельная работа, всего	Контроль	
			Лекции	Лабораторные работы	Практические занятия	Консультации			

1. Основы информационной безопасности	22	16	8		8		6		ОПК- 3.1, ОПК- 3.2
2. Угрозы информационной безопасности	18	12	6	2	4		6		ОПК- 3.1, ОПК- 3.2
3. Основы защиты информационных ресурсов. Построение системы информационной	12	8	4	4			4		ОПК- 3.1, ОПК- 3.2
4. Обеспечение информационной безопасности информационных и	43	36	18	12	6		7		ОПК- 3.1, ОПК- 3.2
5. Консультации	4	4				4			ОПК- 3.1, ОПК- 3.2
ВСЕГО	108	76	36	18	18	4	23	9	

9 семестр заочная форма обучения

Раздел/тема дисциплины, содержание	Всего, час	Объем часов (по видам учебных занятий)							Код индикатора достижения компетенции
		Всего, час	Контактная работа (по учебным занятиям), час				Самостоятельная работа, всего	Контроль	
			Лекции	Лабораторные работы	Практические занятия	Консультации			
1. Основы информационной безопасности	24	2	2				22		ОПК- 3.1, ОПК- 3.2
2. Угрозы информационной безопасности	26	2		2			24		ОПК- 3.1, ОПК- 3.2
3. Основы защиты информационных ресурсов. Построение системы информационной безопасности	24	2	2				22		ОПК- 3.1, ОПК- 3.2
4. Обеспечение информационной безопасности информационных и	26	2			2		24		ОПК- 3.1, ОПК- 3.2
5. Консультации	4	4				4			ОПК- 3.1, ОПК- 3.2
ВСЕГО	108	12	4	2	2	4	92	4	

Формы текущего контроля – посещение и работа на лекционных занятиях и лабораторных работах (собеседование, контрольная работа, круглый стол и дискуссия, отчет по лабораторной работе), письменное задание (реферат), практическое задание (кейс).

Форма промежуточной аттестации – зачёт.

4.2. Содержание дисциплины, структурированное по разделам (темам)

Тема 1. Основы информационной безопасности

Лекционные занятия 1.

Основные понятия и общеметодологические принципы теории информационной безопасности.

Источники понятий в области информационной безопасности. Основные понятия информационной безопасности: документированная информация, безопасность информации, конфиденциальность, целостность, доступность информации, защита информации, система защиты информации. Общеметодологические принципы теории информационной безопасности. Составляющие информационной безопасности.

Практические занятия 2.

Вопросы для обсуждения:

1. Информация как предмет защиты.
2. Субъекты информационных отношений.
3. Задачи обеспечения информационной безопасности.
4. Функции обеспечения информационной безопасности.
5. Составляющие информационной безопасности.

Лекционные занятия 3.

Понятие и сущность защищаемой информации.

Права и обязанности обладателя информации. Виды защищаемой информации: государственная тайна, служебная тайна, профессиональная тайна, коммерческая тайна, персональные данные. Перечень сведений конфиденциального характера. Понятие интеллектуальной собственности и особенности ее защиты. Определение и нормативное закрепление состава защищаемой информации.

Практические занятия 4.

Вопросы для обсуждения:

1. Виды и свойства защищаемой информации.
2. Информация с ограниченным доступом информация.
3. Информация без права ограничения.
4. Иная общедоступная информация.
5. Информация, запрещенная к распространению.
6. Несанкционированный доступ к информации.
7. Факторы, воздействующие на защищаемую информацию.
8. Составление таблицы "Факторы, воздействующие на защищаемую информацию" (объективные - необъективные факторы, внешние - внутренние факторы).
9. Законодательные акты о защите информации в РФ.

Лекционные занятия 5.

Организация системы защиты информации. Составляющие системы защиты информации. Комплексная защита информационных систем. Технологии построения системы защиты. Требования к системе защиты информации. Обзор методов защиты информации. Критерии выборов методов и средств обеспечения информационной безопасности информационных систем.

Лекционные занятия 6.

Критерии безопасности компьютерных систем «Оранжевая книга». Руководящие документы Гостехкомиссии (ФСТЭК) России. Стандарты по управлению информационной безопасностью ISO/IEC 27000.

Практические занятия 7.

Вопросы для обсуждения:

1. Международные стандарты.
2. Государственные (национальные) стандарты РФ.
3. Руководящие документы.

4. Нормативные документы.

Контрольная работа по разделу "Основы информационной безопасности".

Тема 2. Угрозы информационной безопасности

Лекционные занятия 1.

Понятие и виды угроз информационной безопасности. Понятие угрозы информационной безопасности. Фактор, воздействующий на защищаемую информацию. Типы дестабилизирующих факторов. Классификация и виды угроз информационной безопасности. Внутренние и внешние источники угроз информационной безопасности. Угрозы утечки информации и угрозы несанкционированного доступа. Основные элементы канала реализации угрозы безопасности информации. Метод социальной инженерии как способ получения конфиденциальной информации.

Занятие организуется в форме лекции-дискуссии. По ходу лекции-дискуссии преподаватель приводит отдельные примеры в виде ситуаций или кратко сформулированных проблем и предлагает студентам коротко обсудить, затем краткий анализ, выводы и лекция продолжается.

Практические занятия 2.

Вопросы для обсуждения:

1. Модель поведения нарушителя.
2. Классификация угроз.
3. Угрозы утечки по техническим каналам.
4. Угрозы уязвимости каналов взаимодействия.
5. Оценка угроз по классам нарушителей.

Лабораторные занятия 3.

Анализ видов угроз безопасности информации и изучение технологии работы с программами выявления угроз уязвимости каналов взаимодействия:

- Анализ сетевого трафика;
- Сканирование сети;
- Угрозы выявления пароля;
- Распространение вредоносных программ и удаленный запуск.

Лекционные занятия 4.

Информационная безопасность и информационное противоборство. Субъекты информационного противоборства. Цели информационного противоборства. Составные части и методы информационного противоборства. Информационное оружие, его классификация и возможности.

Практические занятия 5.

Вопросы для обсуждения:

1. Методы нарушения конфиденциальности, целостности и доступности информации.
2. Причины, виды, каналы утечки и искажения информации.
3. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны.
4. Компьютерная система как объект информационной войны.

Контрольная работа по разделу "Угрозы информационной безопасности".

Тема 3. Основы защиты информационных ресурсов. Построение системы информационной безопасности

Лекционные занятия 1.

Ключевые аспекты защиты информационных ресурсов. Основные аспекты построения системы информационной безопасности. Программа информационной безопасности. Модели информационной безопасности, требования и основные этапы реализации информационной безопасности. Мероприятия по защите информации законодательного, организационного и программно-технического характера. Политика информационной безопасности. Анализ и управление рисками при реализации информационной безопасности.

Лабораторные занятия 2.

1 часть. Формирование требований к системе информационной безопасности. Определение и описание основных этапов обеспечения информационной безопасности.

2 часть. Моделирование ситуации (на конкретном примере построения системы защиты). Предложений мероприятий по защите информации в нормативно-законодательном аспекте, в организационном аспекте, в процедурном аспекте, в программно-техническом аспекте.

Тема 4. Обеспечение информационной безопасности информационных и компьютерных систем

Лекционные занятия 1.

Информационная система как объект информационной безопасности. Методы и средства обеспечения информационной безопасности информационных и компьютерных систем. Методы и средства обеспечения информационной безопасности компьютерных систем. Общая характеристика способов и средств защиты информации. Правовая, техническая, криптографическая, физическая защита информации. Организационно-правовые, технические и криптографические методы обеспечения информационной безопасности. Программно- аппаратные средства обеспечения информационной безопасности.

Практические занятия 2.

Вопросы для обсуждения:

1. Организационно-техническая составляющая информационной безопасности.
2. Защита информационной инфраструктуры от несанкционированного доступа.
3. Методы обеспечения информационной безопасности информационных и компьютерных систем.
4. Средства обеспечения информационной безопасности компьютерных систем.

Лекционные занятия 3.

Классификация алгоритмов криптографических методов. Методы полиалфавитной замены. Скремблирование потока данных. Двуключевые системы шифрования. Шифрование на базе клеточных автоматов. Использование плавающего окна.

Лабораторные занятия 4.

1 часть. Выполнение практических заданий на шифрование/дешифрование сообщений различными методами.

2 часть. Составление алгоритма и написание программы шифрования/дешифрования.

Занятие проводится в интерактивной форме (работа в парах), что позволяет развивать навыки межличностной коммуникации, командной работы и принятия решений. Каждой паре преподаватель выдает набор исходных данных для выполнения практических заданий (сообщения, которые необходимо расшифровать/зашифровать). По одному из методов шифрования студентам предлагается написать программу.

Лекционные занятия 5.

Механизмы защиты информации в автоматизированных системах. Содержание сервисов безопасности программно-технического уровня. Идентификация и аутентификация, управление доступом и авторизация, протоколирование и аудит. Криптография для сервисов безопасности: шифрование и контроль целостности. Экранирование. Анализ защищенности. Обеспечение доступности. Туннелирование. Управление. Назначение формальных моделей безопасности. Политика безопасности. Монитор безопасности обращений. Дискреционная и мандатная модели безопасности.

Практические занятия 6.

Вопросы для обсуждения:

1. Защита информации, обрабатываемой в автоматизированных системах от технических разведок.
2. Классификация и возможности технических разведок.

3. Компьютерная разведка.

4. Технические каналы утечки информации при эксплуатации автоматизированных систем.

5. Электромагнитное воздействие и эффекты его воздействия.

6. Защита автоматизированных систем и средств вычислительной техники от внешнего электромагнитного воздействия.

Лекционные занятия 7.

Программные средства защиты ИС. Программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации (временных файлов), тестового контроля системы защиты. Типовые схемы идентификации и аутентификации. Протоколы идентификации и аутентификации для типовых схем. Применение пароля для аутентификации пользователя. Основные варианты построения биометрических систем идентификации и аутентификации пользователей. Технические средства биометрической идентификации и аутентификации пользователей.

Практические занятия 8.

Анализ программных средств защиты ИС. Составление классификационной схемы и таблицы (наименование, назначение, применение, примеры программ).

Практическое занятие проводится в парах, что позволяет развивать навыки межличностной коммуникации, командной работы и принятия решений.

Лабораторные занятия 9.

Защита информации средствами офисных приложений.

1. Создание защищенных текстовых документов.
2. Создание защищенных электронных таблицы.
3. Создание защищенных баз данных.

Лекционные занятия 10.

Механизмы контроля доступа. Средства контроля и управления доступом в ИС. Компоненты ОС для защиты информации.

Лабораторные занятия 11.

Защита информации средствами ОС.

1. Защита средствами ОС: авторизация, настройка доступа.
2. Защита информации встроенными средствами BIOS.
3. Управление пользователями и группами в ОС.

Лекционные занятия 12.

Механизмы цифровой подписи. Однонаправленные хэш-функции. Российский стандарт хэш-функции. ГОСТ Р34.11-94. Российский стандарт цифровой подписи. ГОСТ Р 34.10 – 2001.

Лабораторные занятия 13.

Однонаправленные хэш-функции. Системы шифрования с открытым ключом как основа построения систем электронной цифровой подписи.

Лекционные занятия 14.

Обеспечение интегральной безопасности информационных систем и сетей. Критерии оценки защищенности и обеспечения безопасности автоматизированных систем. Анализ соответствия комплексной системы защиты информационной системы требованиям информационной безопасности для предприятия малого бизнеса.

Лабораторные занятия 15.

Выбор методов и средств обеспечения информационной безопасности компьютерной системы. Выбор сервисных программ, в частности антивирусного программного обеспечения. Настройка, обновление и использование антивирусных программ.

5. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

5.1. Виды и организация самостоятельной работы обучающихся

Успешное освоение теоретического материала по дисциплине «Информационная безопасность ИС» требует самостоятельной работы, нацеленной на усвоение лекционного теоретического материала, расширение и конкретизацию знаний по разнообразным вопросам в области информационной безопасности информационных систем, подходов к анализу угроз информационной безопасности.

Самостоятельная работа студентов предусматривает следующие виды:

1. Аудиторная самостоятельная работа студентов – выполнение на практических занятиях и лабораторных работах заданий, закрепляющих полученные теоретические знания либо расширяющие их, а также выполнение разнообразных контрольных заданий индивидуального или группового характера (подготовка устных докладов или сообщений о результатах выполнения заданий, выполнение самостоятельных проверочных работ по итогам изучения от-дельных вопросов и тем дисциплины);

2. Внеаудиторная самостоятельная работа студентов – подготовка к лекционным, практическим занятиям, лабораторным работам, повторение и закрепление ранее изученного теоретического материала, конспектирование учебных пособий и периодических изданий, изучение проблем, не выносимых на лекции, написание тематических рефератов, выполнение индивидуальных практических заданий, подготовка к тестированию по дисциплине, выполнение итоговой работы.

Большое значение в преподавании дисциплины отводится самостоятельному поиску студентами информации по отдельным теоретическим и практическим вопросам и проблемам.

При планировании и организации времени для изучения дисциплины необходимо руководствоваться п. 4.1.1 или 4.1.2 рабочей программы дисциплины «Информационная безопасность ИС» и обеспечить последовательное освоение теоретического материала по отдельным вопросам и темам.

Наиболее целесообразен следующий порядок изучения теоретических вопросов по дисциплине «Информационная безопасность ИС»:

1. Изучение справочников (словарей, энциклопедий) с целью уяснения значения основных терминов, понятий, определений;

2. Изучение учебно-методических материалов для лекционных занятий, лабораторных работ;

3. Изучение рекомендуемой основной и дополнительной литературы и электронных информационных источников;

4. Изучение дополнительной литературы и электронных информационных источников, определенных в результате самостоятельного поиска информации;

5. Самостоятельная проверка степени усвоения знаний по контрольным вопросам и/или заданиям;

6. Повторное и дополнительное (углубленное) изучение рассмотренного вопроса (при необходимости).

В процессе самостоятельной работы над учебным материалом рекомендуется составить конспект, где кратко записать основные положения изучаемой темы. Переходить к следующему разделу можно после того, когда предшествующий материал понят и усвоен. В затруднительных случаях, встречающихся при изучении курса, необходимо обратиться за консультацией к преподавателю.

При изучении дисциплины не рекомендуется использовать материалы, подготовленные неизвестными авторами, размещенные на неофициальных сайтах неделового содержания. Желательно, чтобы используемые библиографические источники были изданы в последние 3-5 лет. Студенты при выполнении самостоятельной работы могут воспользоваться учебно-

методическими материалами по дисциплине «Информационная безопасность ИС», представленными в электронной библиотеке института, и предназначенными для подготовки к лекционным, практическим занятиям и лабораторным работам.

Перечень основных учебно-методических материалов для лекционных, практических занятий и лабораторных работ представлен в п. 7. рабочей программы дисциплины.

Контроль аудиторной самостоятельной работы осуществляется в форме дискуссии, собеседования, защиты отчета по лабораторной работе. Контроль внеаудиторной самостоятельной работы студентов осуществляется в форме устного или письменного опроса.

Промежуточный контроль знаний в форме зачета осуществляется посредством письменного тестирования, включающего вопросы и задания для самостоятельного изучения.

Тема, раздел	Очная форма	Заочная форма	Задания для самостоятельной работы	Форма контроля
1. Основы информационной безопасности	6	22	- изучение проблем, не выносимых на лекции; - подготовка к лабораторным работам; - подготовка тематических рефератов и презентаций; - подготовка к тесту.	- дополненный конспект; - практическое задание; - отчет по лабораторной работе; - реферат;
2. Угрозы информационной безопасности	6	24	- изучение проблем, не выносимых на лекции; - подготовка к лабораторным работам; - подготовка тематических рефератов и презентаций; - подготовка к тесту.	- дополненный конспект; - практическое задание; - отчет по лабораторной работе; - реферат;
3. Основы защиты информационных ресурсов. Построение системы информационной безопасности	4	22	- изучение проблем, не выносимых на лекции; - подготовка к лабораторным работам; - подготовка тематических рефератов и презентаций; - подготовка к тесту.	- дополненный конспект; - практическое задание; - отчет по лабораторной работе; - реферат;
4. Обеспечение информационной безопасности информационных и компьютерных систем	7	24	- изучение проблем, не выносимых на лекции; - подготовка к лабораторным работам; - подготовка тематических рефератов и презентаций; - примеры программ для защиты домашнего ПК; - подготовка к тесту.	- дополненный конспект; - практическое задание; - отчет по лабораторной работе; - реферат;
ИТОГО	23	92		

5.2. Учебно-методическое обеспечение самостоятельной работы обучающихся

Учебно-методическое обеспечение самостоятельной работы обучающихся отражено в п.7 рабочей программы дисциплины «Информационная безопасность ИС».

6. КОМПЛЕКТЫ ОЦЕНОЧНЫХ МАТЕРИАЛОВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

6.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Освоение дисциплины направлено на формирование:
общепрофессиональных компетенций

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

Данные компетенции формируются в процессе изучения дисциплины на двух этапах:
этап 1 – текущий контроль;
этап 2 – промежуточная аттестация.

6.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Оценка компетенций на различных этапах их формирования осуществляется в соответствии с Положением о текущем контроле и промежуточной аттестации, Положением о балльной и рейтинговой системах оценивания и технологической картой дисциплины (Приложение 1), принятыми в Институте.

6.2.1. Показатели и критерии оценивания компетенций на этапе текущего контроля

№ п/п	Показатели оценивания	Критерии оценивания	Шкала оценивания
1	Посещение и работа на лекционных и практических занятиях (собеседование, контрольная работа, круглый стол и дискуссия)	1. Посещение занятий: а) посещение лекционных и практических занятий, б) соблюдение дисциплины. 2. Работа на лекционных занятиях: а) ведение конспекта лекций, б) уровень освоения теоретического материала, в) активность на лекции, умение формулировать вопросы лектору. 3. Работа на практических занятиях: а) уровень знания учебно-программного материала, б) умение выполнять задания, предусмотренные программой курса, в) практические навыки работы с освоенным материалом.	0-35
2	Письменное задание	1. Новизна текста: а) актуальность темы исследования; б) новизна и самостоятельность в постановке проблемы, формулирование нового аспекта известной проблемы в установлении новых связей (межпредметных, внутрипредметных, интеграционных); в) умение работать с исследованиями, критической литературой, систематизировать и структурировать материал; г) явленность авторской позиции, самостоятельность оценок и суждений; д) стилевое единство текста, единство жанровых черт.	0-25

		2. Степень раскрытия сущности вопроса: а) соответствие плана теме письменного задания; б) соответствие содержания теме и плану письменного задания; в) полнота и глубина знаний по теме; г) обоснованность способов и методов работы с материалом; д) умение обобщать, делать выводы, сопоставлять различные точки зрения по одному вопросу (проблеме). 3. Обоснованность выбора источников: а) оценка использованной литературы: привлечены ли наиболее известные работы по теме исследования (в т.ч. журнальные публикации последних лет, последние статистические данные, сводки, справки и т.д.). 4. Соблюдение требований к оформлению: а) насколько верно оформлены ссылки на используемую литературу, список литературы; б) оценка грамотности и культуры изложения (в т.ч. орфографической, пунктуационной, стилистической культуры), владение терминологией; в) соблюдение требований к объёму письменного задания.	
3	Практическое задание	1. Анализ проблемы: а) умение верно, комплексно и в соответствии с действительностью выделить причины возникновения проблемы, описанной в практическом задании. 2. Структурирование проблем: а) насколько четко, логично, последовательно были изложены проблемы, участники проблемы, последствия проблемы, риски для объекта. 3. Предложение стратегических альтернатив: а) количество вариантов решения проблемы, б) умение связать теорию с практикой при решении проблем. 4. Обоснование решения: а) насколько аргументирована позиция относительно предложенного решения практического задания; б) уровень владения профессиональной терминологией. 5. Логичность изложения материала: а) насколько соблюдены общепринятые нормы логики в предложенном решении, б) насколько предложенный план может быть реализован в текущих условиях.	0-50

6.2.2. Показатели и критерии оценивания компетенций на этапе промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме зачёта в виде выполнения тестирования и/или итоговой работы.

Итоговые задания разрабатываются по основным вопросам теоретического материала и позволяют осуществлять промежуточный контроль знаний и степени усвоения материала.

При проведении промежуточной аттестации студентов по дисциплине «Информационная безопасность ИС» могут формироваться варианты тестов, относящихся ко всем темам дисциплины.

Оценка знаний студентов осуществляется в соответствии с Положением о балльной и рейтинговой системах оценивания, принятой в Институте, и технологической картой дисциплины

№ п/п	Показатели оценивания	Критерии оценивания	Шкала оценивания
1	Итоговая работа	Количество баллов за тест пропорционально количеству правильных ответов на тестовые задания. После прохождения теста суммируются результаты выполнения всех заданий для выставления общей оценки за тест.	0-25

6.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

6.3.1. Типовые контрольные задания или иные материалы на этапе текущего контроля

Посещение и работа на лекционных и практических занятиях (собеседование, контрольная работа, круглый стол и дискуссия)

При преподавании дисциплины «Информационная безопасность ИС» применяются разнообразные образовательные технологии в зависимости от вида и целей учебных занятий.

Теоретический материал излагается на лекционных занятиях в следующих формах:

- проблемные лекции;
- лекция-беседа.

Лабораторные работы и практические занятия по дисциплине «Информационная безопасность ИС» ориентированы на закрепление теоретического материала, изложенного на лекционных занятиях, а также на приобретение дополнительных знаний, умений и практических навыков осуществления профессиональной деятельности посредством активизации и усиления самостоятельной деятельности обучающихся.

Лабораторные работы и практические занятия проводятся с применением активных форм обучения, к которым относятся:

1) интерактивные задания (например, тренажеры);

2) групповая работа студентов, предполагающая совместное обсуждение какой-либо проблемы (вопроса) и выработку единого мнения (позиции) по ней (метод группового обсуждения);

3) контрольная работа по отдельным вопросам, целью которой является проверка знаний студентов и уровень подготовленности для усвоения нового материала по дисциплине.

На практических занятиях оцениваются и учитываются все виды активности студентов: устные ответы, дополнения к ответам других студентов, участие в дискуссиях, работа в группах, инициативный обзор проблемного вопроса, письменная работа.

Более подробно с содержанием лекционных занятий и лабораторных работ можно ознакомиться в п. 4.2 рабочей программы дисциплины «Информационная безопасность ИС».

Письменное задание

(формируемые компетенции: ОПК-3)

Цели и задачи реферата.

Целью работы является обобщение и систематизация теоретического материала в рамках исследуемой проблемы.

В процессе выполнения работы решаются следующие задачи:

1. Формирование информационной базы:

• анализ точек зрений зарубежных и отечественных специалистов;

• конспектирование и реферирование первоисточников в качестве базы для сравнения, противопоставления, обобщения;

• анализ и обоснование степени изученности исследуемой проблемы;

• подготовка библиографического списка исследования.

2. Формулировка актуальности темы:

• отражение степени важности исследуемой проблемы в современной теории и практике;

• выявление соответствия задачам теории и практики, решаемым в настоящее время;

• определение места выбранной для исследования проблемы.

3. Формулировка цели и задач работы:

• изложение того, какой конечный результат предполагается получить при проведении теоретического исследования;

• четкая формулировка цели и разделение процесса ее достижения на этапы;

• выявление особенностей решения задач (задачи - это те действия, которые необходимо предпринять для достижения поставленной в работе цели).

В результате написания реферата студент изучает и анализирует информационную базу с целью установления теоретических зависимостей, формулирует понятийный аппарат, определяет актуальность, цель и задачи работы.

Обязательными составляющими элементами реферата являются:

- титульный лист;
- содержание;
- введение;
- основное содержание, разделенное на разделы (параграфы, пункты, подпункты), расположенные и поименованные согласно плану; в них аргументировано и ло-гично раскрывается избранная тема в соответствии с поставленной целью; обзор литературы; описание применяемых методов, инструментов, методик, процедур в рамках темы исследования; анализ примеров российского и зарубежного опыта, отражающих тему исследования и т.д..
- заключение;
- список использованных источников;
- приложения.

Требования к оформлению практических работ представлены в Методических указаниях к содержанию, оформлению и критериям оценивания письменных, практических и лабораторных работ, утвержденных решением Научно-методического совета (протокол №8 от 07.06.2018 г.).

Номер темы для выполнения реферата определяется по таблице (прил. 2).

Примерная тематика рефератов

1. Информация как предмет защиты.
2. Технические средства защиты информации.
3. Программные средства защиты информации.
4. Организационные средства защиты информации.
5. Законодательные средства защиты информации.
6. Электронная почта и ее защита.
7. Криптографические методы шифрования и их классификация.
8. Частотный анализ как один из методов криптоанализа.
9. Криптографические стандарты DES и ГОСТ 28147-89.
10. Проблемы и перспективы криптографических систем.

11. Виды вирусов, их классификации и методы борьбы с вирусами.
12. Специализированные программы для защиты от вирусов.
13. Защита информации в компьютерных сетях.
14. Методы борьбы с фишинговыми атаками.
15. Утечки информации: как избежать. Безопасность смартфонов.
16. Антишпионское ПО (antispyware).
17. Обеспечение безопасности Web-сервисов информационных систем.
18. Защита информационных систем от внутренних угроз.
19. Ботнеты - плацдарм современных кибератак.
20. Критерии оценки защищенности и обеспечения безопасности автоматизированных систем.
21. Основные требования информационной безопасности.
22. Защита информации от утечки на объектах информатизации.
23. Системы разграничения доступа к информации.
24. Защита информации в телекоммуникационных системах.
25. Юридическая ответственность за нарушение норм в области информационной безопасности.

Практическое задание

(формируемые компетенции: ОПК-3)

Расчетно-графическое задание

Задание:
1. Проанализировать угрозы. Рассчитать исходную защищенность.
2. Обосновать выбор методов и средств обеспечения информационной безопасности (программные, технические, организационные средства).

Исходные данные для выполнения задания и варианты заданий представлены в прил. 3.

Ход выполнения работы
1. Выберите вариант практического задания (прил. 3).
2. Проанализируйте исходные данные.
3. Рассчитайте исходную защищенность.
4. Обоснуйте выбор методов и средств обеспечения информационной безопасности (программные, технические, организационные средства).

Отчет по выполнению практического задания должен содержать титульный лист и описание выполненного задания (цели, задачи; номер варианта; исходные данные; описание пунктов хода выполнения работы; заключение с выводами).

Требования к оформлению практических работ представлены в Методических указаниях к содержанию, оформлению и критериям оценивания письменных, практических и лабораторных работ, утвержденных решением Научно-методического совета (протокол №8 от 07.06.2018 г.).

6.3.2. Типовые контрольные задания или иные материалы на этапе промежуточной аттестации

(формируемые компетенции: ОПК-3)

Тестовые задания представлены в приложении 4.

Примерный перечень вопросов к зачету по дисциплине "Информационная безопасность ИС"

1. Основные понятия и общеметодологические принципы теории информационной безопасности.
2. Составляющие информационной безопасности.

3. Понятие и сущность защищаемой информации. Права и обязанности обладателя информации.

4. Виды защищаемой информации: государственная тайна, служебная тайна, профессиональная тайна, коммерческая тайна, персональные данные. Перечень сведений конфиденциального характера.

5. Понятие интеллектуальной собственности и особенности ее защиты.

6. Определение и нормативное закрепление состава защищаемой информации.

7. Организация системы защиты информации. Составляющие системы защиты информации.

8. Комплексная защита информационных систем.

9. Технологии построения системы защиты.

10. Требования к системе защиты информации.

11. Обзор методов защиты информации.

12. Критерии выборов методов и средств обеспечения информационной безопасности информационных систем.

13. Критерии безопасности компьютерных систем «Оранжевая книга».

14. Руководящие документы Гостехкомиссии (ФСТЭК) России.

15. Стандарты по управлению информационной безопасностью ISO/IEC 27000.

16. Понятие и виды угроз информационной безопасности.

17. Типы дестабилизирующих факторов. Классификация и виды угроз информационной безопасности.

18. Внутренние и внешние источники угроз информационной безопасности.

19. Метод социальной инженерии как способ получения конфиденциальной информации.

20. Информационная безопасность и информационное противоборство. Субъекты информационного противоборства. Цели информационного противоборства. Составные части и методы информационного противоборства.

21. Информационное оружие, его классификация и возможности.

22. Ключевые аспекты защиты информационных ресурсов.

23. Основные аспекты построения системы информационной безопасности.

24. Модели информационной безопасности, требования и основные этапы реализации информационной безопасности.

25. Мероприятия по защите информации законодательного, организационного и программно-технического характера. Политика информационной безопасности.

26. Информационная система как объект информационной безопасности.

27. Методы и средства обеспечения информационной безопасности информационных и компьютерных систем.

28. Общая характеристика способов и средств защиты информации.

29. Организационно-правовые, технические и криптографические методы обеспечения информационной безопасности.

30. Программно-аппаратные средства обеспечения информационной безопасности.

31. Классификация алгоритмов криптографических методов.

32. Методы полиалфавитной замены.

33. Скремблирование потока данных.

34. Двуключевые системы шифрования.

35. Шифрование на базе клеточных автоматов.

36. Использование плавающего окна.

37. Механизмы защиты информации в автоматизированных системах.

38. Содержание сервисов безопасности программно-технического уровня. Идентификация и аутентификация, управление доступом и авторизация, протоколирование и аудит

39. Политика безопасности.

40. Механизмы контроля доступа.

41. Средства контроля и управления доступом в ИС.

42. Компоненты ОС для защиты информации.

43. Механизмы цифровой подписи. Однонаправленные хэш-функции.

44. Российский стандарт хэш-функции. ГОСТ Р34.11-94. Российский стандарт цифровой подписи. ГОСТ Р 34.10 – 2001.

45. Обеспечение интегральной безопасности информационных систем и сетей.

46. Критерии оценки защищенности и обеспечения безопасности автоматизированных систем.

47. Анализ соответствия комплексной системы защиты информационной системы требованиям информационной безопасности для предприятия малого бизнеса.

Типовые практические задания на этапе промежуточной аттестации
(формируемые компетенции: ОПК-3)

Для заданной предметной области:

1. Проанализировать виды угроз безопасности информационной системы.

2. Выбрать методы и средства обеспечения информационной безопасности информационной системы.

3. Перечислить необходимые программные, технические, организационные средства обеспечения информационной безопасности.

Примечание. Выбор варианта выполняется по таблице (прил. 5).

Описание предметных областей:

Вариант 1

Исходные данные: финансовая структура, имеющая систему дистанционного банковского обслуживания физических и юридических лиц. Структура распределенная.

Вариант 2

Исходные данные: финансовая структура, имеющая систему дистанционного банковского обслуживания физических и юридических лиц. Структура нераспределенная.

Вариант 3

Исходные данные: локальная структурирования кабельная сеть предприятия, в состав сети входят 10 ЭВМ, 20 телефонов и 6 камер видеонаблюдения.

Вариант 4

Исходные данные: локальная структурированная кабельная сеть предприятия, в состав сети входят 50 ЭВМ, 25 телефонов, 15 камер видеонаблюдения.

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

Процедура оценивания знаний, умений, навыков и (или) опыта деятельности обучающихся по дисциплине «Информационная безопасность ИС» основана на использовании Положения о балльной и рейтинговой системах оценивания, принятой в институте, и технологической карты дисциплины.

№ п/п	Показатели оценивания	Шкала оценивания
Текущий контроль		
1	Посещение и работа на лекционных и практических занятиях (собеседование, контрольная работа, круглый стол и дискуссия)	0-35
2	Письменное задание (реферат)	0-25
3	Практическое задание (кейс)	0-50
	Итого текущий контроль	75
Промежуточная аттестация		
4	Итоговая работа	25
	Итого промежуточная аттестация	25
	ИТОГО по дисциплине	**100**

Максимальное количество баллов по дисциплине – 100.
Максимальное количество баллов по результатам текущего контроля – 75.
Максимальное количество баллов на экзамене – 25.

Уровень подготовленности обучающегося соответствует трехуровневой оценке компетенций в зависимости от набранного количества баллов по дисциплине.

	Уровень овладения		
	Пороговый уровень	**Продвинутый уровень**	**Превосходный уровень**
Набранные баллы	50-69	70-85	86-100

Шкала итоговых оценок успеваемости по дисциплине «Информационная безопасность ИС» соответствует Положению о балльной и рейтинговой системах оценивания и отражена в технологической карте дисциплины.

Зачёт

Количество баллов	**Оценка**
50-100	зачтено
0-49	не зачтено

Экзамен

Количество баллов	**Оценка**
86-100	отлично
70-85	хорошо
50-69	удовлетворительно
0-49	неудовлетворительно

7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Основная литература:

1. Моргунов А. В. Информационная безопасность [Электронный ресурс]:учебно-методическое пособие. - Новосибирск: Новосибирский государственный технический университет, 2019. - 83 с. – Режим доступа: https://biblioclub.ru/index.php?page=book&id=576726

2. Марухленко А. Л., Марухленко Л. О., Ефремов М. А., Таныгин М. О., Кулешова Е. А. Технологии обеспечения безопасности информационных систем [Электронный ресурс]:учебное пособие. - Москва, Берлин: Директ-Медиа, 2021. - 210 с. – Режим доступа: https://biblioclub.ru/index.php?page=book&id=598988

Дополнительная литература:

1. Громов Ю. Ю., Иванова О. Г., Стародубов К. В., Кадыков А. А. Программно- аппаратные средства защиты информационных систем [Электронный ресурс]:учебное пособие. - Тамбов: Тамбовский государственный технический университет (ТГТУ), 2017. - 194 с. – Режим доступа: https://biblioclub.ru/index.php?page=book&id=499013

2. Басыня Е. А. Системное администрирование и информационная безопасность [Электронный ресурс]:учебное пособие. - Новосибирск: Новосибирский государственный технический университет, 2018. - 79 с. – Режим доступа: https://biblioclub.ru/index.php?page=book&id=575325

3. Бобынцев Д. О., Марухленко А. Л., Марухленко Л. О., Кужелева С. А., Лисицын Л. А. Основы администрирования информационных систем [Электронный ресурс]:учебное пособие. - Москва, Берлин: Директ-Медиа, 2021. - 201 с. – Режим доступа: https://biblioclub.ru/index.php?page=book&id=598955

4. Рогозин В. Ю., Галушкин И. Б., Новиков В., Вепрев С. Б. Основы информационной безопасности [Электронный ресурс]:учебник. - Москва: Юнити-Дана|Закон и право, 2018. - 287 с. – Режим доступа: https://biblioclub.ru/index.php?page=book&id=562348

5. Ищейнов В. Я. Информационная безопасность и защита информации: теория и практика [Электронный ресурс]:учебное пособие. - Москва, Берлин: Директ-Медиа, 2020. - 271 с. – Режим доступа: https://biblioclub.ru/index.php?page=book&id=571485

6. Закарюкин В. П., Дмитриева М. Л., Крюков А. В. Электромагнитная совместимость и средства защиты [Электронный ресурс]:учебное пособие. - Москва, Берлин: Директ-Медиа, 2020. - 248 с. – Режим доступа: https://biblioclub.ru/index.php?page=book&id=598053

8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО- ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ "ИНТЕРНЕТ", НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Информационные ресурсы образовательной организации:

1. http://www.sibit.sano.ru/ - официальный сайт образовательной организации.
2. http://do.sano.ru - система дистанционного обучения Moodle (СДО Moodle).
3. http://window.edu.ru/ - Информационная система «Единое окно доступа к образовательным ресурсам».
4. http://uisrussia.msu.ru/is4/main.jsp - Университетская информационная система РОССИЯ.
5. http://www.ebiblioteka.ru/ - базы данных East View.
6. http://www.edu.ru - Федеральный портал «Российское образование».
7. http://www.encyclopedia.ru - Мир энциклопедий.
8. https://scholar.google.ru - международная научная реферативная база данных.
9. https://academic.microsoft.com - международная научная реферативная база данных.
10. http://crypt-online.ru/ - онлайн-средство шифрования.
11. https://www.kaspersky.ru/ - официальный сайт компании «Лаборатория Касперского».
12. https://www.esetnod32.ru/ - официальный сайт компании «ESET».

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

В процессе изучения учебной дисциплины «Информационная безопасность ИС» следует:

1. Ознакомиться с рабочей программой дисциплины. Рабочая программа содержит перечень разделов и тем, которые необходимо изучить, планы лекционных и практических занятий, вопросы к текущей и промежуточной аттестации, перечень основной, дополнительной литературы и ресурсов информационно-коммуникационной сети «Интернет» и т.д.
2. Ознакомиться с календарно-тематическим планом самостоятельной работы обучающихся.
3. Посещать теоретические (лекционные) занятия, практические занятия, лабораторные работы.
4. При подготовке к лабораторным работам и практическим занятиям, а также при выполнении самостоятельной работы следует использовать методические указания для обучающихся.

Учебный план курса «Информационная безопасность ИС» предполагает в основе изучения предмета использовать лекционный материал и основные источники литературы, а в дополнение – методические материалы к лабораторным работами практическим занятиям.

Кроме традиционных лекций, практических занятий (перечень и объем которых указаны) целесообразно в процессе обучения использовать и активные формы обучения.

Примерный перечень активных форм обучения:

1) беседы и дискуссии;
2) кейсы и практические ситуации;
3) индивидуальные творческие задания;
4) интерактивные задания в группах;
5) практические задания (проекты).

На лекциях студенты должны получить систематизированный материал по теме занятия: основные понятия и положения, классификации изучаемых явлений и информационных процессов и т.д.

Лабораторные работы и практические занятия предполагают более детальную проработку темы по каждой изучаемой проблеме, анализ теоретических и практических аспектов информационной безопасности ИС. Для этого разработаны практические задания, темы рефератов и тесты. При подготовке к практическим занятиям следует акцентировать внимание на значительную часть самостоятельной практической работы студентов.

Для более успешного изучения курса преподавателю следует постоянно отсылать студентов к учебникам, периодической печати. Освоение всех разделов курса предполагает приобретение студентами умений самостоятельного анализа инструментов и механизмов информационных и коммуникационных технологий, умение работать с научной литературой.

При изучении курса наряду с овладением студентами теоретическими положениями курса уделяется внимание приобретению практических умений с тем, чтобы они смогли успешно применять их в своей профессиональной деятельности.

Большое значение при проверке знаний и умений придается тестированию и подготовке рефератов по темам курса.

Активные формы проведения занятий открывают большие возможности для проверки усвоения теоретического и практического материала.

Основная учебная литература, представленная учебниками и учебными пособиями, охватывает все разделы программы по дисциплине «Информационная безопасность ИС». Она изучается студентами в процессе подготовки к практическим занятиям, зачету. Дополнительная учебная литература рекомендуется для самостоятельной работы по подготовке к практическим занятиям, при написании рефератов.

10. СОВРЕМЕННЫЕ ПРОФЕССИОНАЛЬНЫЕ БАЗЫ ДАННЫХ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

При подготовке и проведении учебных занятий по дисциплине студентами и преподавателями используются следующие современные профессиональные базы данных и информационно-справочные системы:

1. Электронная библиотечная система «Университетская библиотека онлайн» (договор № 109-08/2021 на оказание услуг по предоставлению доступа к электронным изданиям базовой коллекции ЭБС «Университетская библиотека онлайн» от 01 сентября 2021 г. (http://www.biblioclub.ru).

2. Интегрированная библиотечно-информационная система ИРБИС64 (договор № С 2-08 - 20 о поставке научно-технической продукции – Системы Автоматизации Библиотек ИРБИС64 – от 19 августа 2020 г., в состав которой входит База данных электронного каталога библиотеки СИБИТ Web-ИРБИС 64 (http://lib.sano.ru).

3. Справочно-правовая система КонсультантПлюс (дополнительное соглашение №1 к договору № 11/01-09 от 01.09.2009).

4. Электронная справочная система ГИС Омск.

11. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ, НЕОБХОДИМОЕ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Для проведения учебных занятий по дисциплине используются следующие помещения, оснащенные оборудованием и техническими средствами обучения:

Наименование учебных аудиторий и помещений для самостоятельной работы	Оснащенность оборудованием и техническими средствами обучения
Мультимедийная учебная аудитория № 210. для проведения занятий лекционного типа, занятий семинарского типа (практических занятий), групповых консультаций, индивидуальных консультаций, текущего контроля, промежуточной аттестации, государственной итоговой аттестации	Учебная мебель (36 столов, 74 стула, доска маркерная, трибуна, стол и стул преподавателя). Мультимедийное демонстрационное оборудование (проектор, экран, компьютер с выходом в Интернет, аудиоколонки - 5шт.) Программное обеспечение: Microsoft Windows XP Professional Russian, Number License: 42024141 OPEN 61960499ZZE0903(коммерческая лицензия, иностранный производитель); Microsoft Office Standart 2007 Win32 Russian, Number License 42024141 OPEN 61960499ZZE0903 (коммерческая лицензия, иностранный производитель); Consultant Plus - Договор 11/01-09 от 01.09.2009 г. Доп.соглашение №1 (автопролонгация) (коммерческая лицензия, отечественный производитель); Adobe Acrobat Reader, лицензия freeware; (свободно распространяемое ПО, иностранный производитель) Kaspersky Endpoint Security - Russian Edition, лицензия № 1356-181109-064939-827-947 (коммерческая лицензия, отечественный производитель ПО); 2GIS, лицензия freeware (свободно распространяемое ПО, отечественный производитель). Обеспечен доступ к сети Интернет и в электронную информационно-образовательную среду организации.
Мультимедийная учебная аудитория № 211. для проведения занятий лекционного типа, занятий семинарского типа (практических занятий), групповых консультаций, индивидуальных консультаций, текущего контроля, промежуточной аттестации, государственной итоговой аттестации	Учебная мебель (27 столов, 54 стула, маркерная доска, трибуна, стол и стул преподавателя). Мультимедийное демонстрационное оборудование (проектор, экран, компьютер с выходом в Интернет, аудиоколонки - 5шт.) Программное обеспечение: Microsoft Windows XP Professional Russian, Number License: 42024141 OPEN 61960499ZZE0903 (коммерческая лицензия, иностранный производитель); Microsoft Office Standart 2007 Win32 Russian, Number License 42024141 OPEN 61960499ZZE0903 (коммерческая лицензия, иностранный производитель); Consultant Plus - Договор 11/01-09 от 01.09.2009 г. Доп.соглашение №1 (автопролонгация); (коммерческая лицензия, отечественный производитель); Adobe Acrobat Reader, лицензия freeware; Kaspersky Endpoint Security - Russian Edition, лицензия № 1356-181109-064939-827-947 (коммерческая лицензия, отечественный производитель ПО); 2GIS, лицензия freeware (свободно распространяемое ПО, отечественный производитель). Обеспечен доступ к сети Интернет и в электронную информационно-образовательную среду организации.

Мультимедийная учебная аудитория № 304. для проведения занятий лекционного типа, занятий семинарского типа (практических занятий), групповых консультаций, индивидуальных консультаций, текущего контроля, промежуточной аттестации, государственной итоговой аттестации	Учебная мебель (22 стола, 44 стула, доска маркерная, трибуна, стол и стул преподавателя). Мультимедийное оборудование (проектор, экран, компьютер с выходом в Интернет, колонки - 2 шт.). Учебно- наглядные пособия. Тематические иллюстрации. Программное обеспечение: Microsoft Windows 10 домашняя для одного языка, ID продукта: 00327-30584-64564-AAOEM; (коммерческая лицензия, иностранный производитель) Microsoft Office Standart 2007 Win32 Russian, Number License 42024141 OPEN 61960499ZZE0903 (коммерческая лицензия, иностранный производитель); Consultant Plus - Договор 11/01 -09 от 01.09.2009 г. Доп.соглашение №1 (автопролонгация) (коммерческая лицензия, отечественный производитель ПО); Adobe Acrobat Reader, лицензия freeware (свободно распространяемое ПО, иностранный производитель); Kaspersky Endpoint Security - Russian Edition, лицензия № 1356-181109- 064939-827-947; 2GIS, лицензия freeware (свободно распространяемое ПО, отечественный производитель). Обеспечен доступ к сети Интернет и в электронную информационно-образовательную среду организации.
Аудитория для самостоятельной работы студентов № 305. помещение для самостоятельной работы обучающихся, научно -исследовательской работы обучающихся, курсового проектирования (выполнения курсовых работ)	Учебная мебель (10 столов одноместных, 3 круглых стола, 27 стульев, доска маркерная, доска информационная, трибуна, стеллаж - 2 шт., стол и стул преподавателя). Мультимедийное оборудование (проектор, экран, компьютер с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Института, колонки - 2 шт.). Ноутбук DELL - 8 шт. Ноутбук HP - 2 шт. Персональный компьютер - 1 шт. СПС «Консультант Плюс». Программное обеспечение: Microsoft Windows 10 Pro Russian, Number License: 69201334 OPEN 99384269ZZE1912 (коммерческая лицензия, иностранный производитель); Microsoft Office 2016 standart Win64 Russian, Number License 67568455 OPEN 97574928ZZE1810 (коммерческая лицензия, иностранный производитель); Consultant Plus - Договор 11/01-09 от 01.09.2009 г. Доп.соглашение №1 (автопролонгация); Adobe Acrobat Reader, лицензия freeware (свободно распространяемое ПО, иностранный производитель); Kaspersky Endpoint Security – Russian Edition, лицензия № 1356-181109-064939-827-947; (коммерческая лицензия, отечественный производитель ПО); 2GIS, лицензия freeware. (свободно распространяемое ПО, отечественный производитель). Обеспечен доступ к сети Интернет и в электронную информационно-образовательную среду организации.

Мультимедийная учебная аудитория № 312. для проведения занятий лекционного типа, занятий семинарского типа (практических занятий), групповых консультаций, индивидуальных консультаций, текущего контроля, промежуточной аттестации, государственной итоговой аттестации	Учебная мебель (50 столов, 100 стульев, доска маркерная, трибуна, стол и стул преподавателя); Мультимедийное оборудование (проектор, экран, компьютер, колонки - 2 шт.). Учебно-наглядные пособия. Тематические иллюстрации. Программное обеспечение: Microsoft Windows XP Professional Russian, Number License: 42024141 OPEN 61960499ZZE0903 (коммерческая лицензия, иностранный производитель); Microsoft Office Standart 2007 Win32 Russian, Number License 42024141 OPEN 61960499ZZE0903 (коммерческая лицензия, иностранный производитель); Consultant Plus - Договор 11/01-09 от 01.09.2009 г. Доп.соглашение №1 (автопролонгация); Adobe Acrobat Reader, лицензия freeware; Kaspersky Endpoint Security - Russian Edition, лицензия № 1356-181109-064939-827-947 (коммерческая лицензия, отечественный производитель ПО); 2GIS, лицензия freeware (свободно распространяемое ПО, отечественный производитель) Обеспечен доступ к сети Интернет и в электронную информационно-образовательную среду организации.
Лаборатория иностранных языков и информационных дисциплин № 401. для проведения занятий семинарского типа (практических занятий и лабораторных работ), групповых консультаций, индивидуальных консультаций, текущего контроля, промежуточной аттестации, государственной итоговой аттестации, научно- исследовательской работы обучающихся, курсового проектирования (выполнения курсовых работ)	Учебная мебель (8 столов, 13 стульев, доска маркерная, доска информационная, стол и стул преподавателя). Персональные компьютеры для работы в электронной образовательной среде с выходом в Интернет - 10 шт. Лингафонное оборудование (компьютер, интерактивная доска, наушники с микрофоном 10 шт., специальное программное обеспечение - JoyClass). Лицензионное программное обеспечение, используемое в учебном процессе. Мультимедиапроектор, интерактивная доска. Учебно-наглядные пособия. Тематические иллюстрации. Программное обеспечение: Russian, NumberLicense: 62668511 OPEN 91741712ZZE1503 (коммерческая лицензия, иностранный производитель); MicrosoftOffice 2016 StandartWin64 Russian, NumberLicense 66020759 OPEN 96028013ZZE1711 (коммерческая лицензия, иностранный производитель); ConsultantPlus - Договор 11/01 -09 от 01.09.2009 г. Доп.соглашение №1 (автопролонгация); AdobeAcrobatReader, лицензия freeware; Kaspersky Endpoint Security - Russian Edition, лицензия № 1356-181109- 064939-827-947; MicrosoftAccess 2016, NumberLicense: 69201333 OPEN 99384269ZZE1912 (коммерческая лицензия, иностранный производитель); JoyClass, Договор №36/15-Л от 26.10.2015 г. СППР "Выбор", Договор № 10 от 06.02.2018 г. NetBeansIDE, лицензия freeware (свободно распространяемое ПО, иностранный производитель); MicrosoftVisualStudio 2017 CE (C#, C++), лицензия freeware (свободно распространяемое ПО, иностранный производитель); MicrosoftVisualStudio 2010 Express, лицензия freeware(свободно распространяемое ПО, иностранный производитель);

	Microsoft Visual Studio Community, лицензия freeware (свободно распространяемое ПО, иностранный производитель); MicrosoftSQL 2010 Express, лицензия freeware (свободно распространяемое ПО, иностранный производитель); Notepad ++, лицензия freeware (свободно распространяемое ПО, иностранный производитель); MySQL, лицензия freeware (свободно распространяемое ПО, иностранный производитель); OracleSQLDeveloper, лицензия freeware; MicrosoftSOAPToolkit, лицензия freeware (свободно распространяемое ПО, иностранный производитель); CADE, лицензия freeware (свободно распространяемое ПО, иностранный производитель); Denwer 3 webserver, лицензия freeware (свободно распространяемое ПО, иностранный производитель); Dev-C++, лицензия freeware; IDEEclipse, лицензия freeware (свободно распространяемое ПО, иностранный производитель); JDK 6, лицензия freeware (свободно распространяемое ПО, иностранный производитель); Freepascal, лицензия freeware (свободно распространяемое ПО, иностранный производитель); Lazarus, лицензия freeware (свободно распространяемое ПО, иностранный производитель); Geany, лицензия freeware (свободно распространяемое ПО, иностранный производитель); JavaDevelopmentKit, лицензия freeware (свободно распространяемое ПО, иностранный производитель); TheRProject, лицензия freeware 9 (свободно распространяемое ПО, иностранный производитель); NetBeansIDE8, лицензия freeware (свободно распространяемое ПО, иностранный производитель); StarUML 5.0.2, лицензия freeware (свободно распространяемое ПО, иностранный производитель); EViews 9 StudentVersionLite, лицензия freeware (свободно распространяемое ПО, иностранный производитель); Gretl, лицензия freeware (свободно распространяемое ПО, иностранный производитель); Matrixer, лицензия freeware (свободно распространяемое ПО, иностранный производитель); Maxima, лицензия freeware (свободно распространяемое ПО, иностранный производитель); Xmind, лицензия freeware (свободно распространяемое ПО, иностранный производитель); BPWIN, лицензия freeware; Gimp, лицензия freeware (свободно распространяемое ПО, иностранный производитель); IrfanView, лицензия freeware (свободно распространяемое ПО, иностранный производитель); SMARTBoard, Акт №ДС – 0001621 от 06.12.12 г., Акт №ДС – 0001620 от 06.12.12 г.; 2GIS, лицензия freeware (свободно распространяемое ПО, отечественный производитель). Обеспечен доступ к сети Интернет и в электронную информационно- образовательную среду организации.

Лаборатория экономических и информационных дисциплин № 402. для проведения занятий семинарского типа (практических занятий и лабораторных работ), групповых консультаций, индивидуальных консультаций, текущего контроля, промежуточной аттестации, государственной итоговой аттестации, научно- исследовательской работы обучающихся, курсового проектирования (выполнения курсовых работ)	Учебная мебель (8 столов, 13 стульев, доска маркерная, доска информационная, стол и стул преподавателя). Персональные компьютеры для работы в электронной образовательной среде с выходом в Интернет - 10 шт. Лингафонное оборудование (компьютер, интерактивная доска, наушники с микрофоном 10 шт., специальное программное обеспечение - JoyClass). Лицензионное программное обеспечение, используемое в учебном процессе. Мультимедиапроектор, интерактивная доска. Учебно-наглядные пособия. Тематические иллюстрации. Программное обеспечение: Russian, NumberLicense: 62668511 OPEN 91741712ZZE1503 (коммерческая лицензия, иностранный производитель); MicrosoftOffice 2016 StandartWin64 Russian, NumberLicense 66020759 OPEN 96028013ZZE1711 (коммерческая лицензия, иностранный производитель); ConsultantPlus - Договор 11/01 -09 от 01.09.2009 г. Доп.соглашение №1 (автопролонгация); AdobeAcrobatReader, лицензия freeware; Kaspersky Endpoint Security - Russian Edition, лицензия № 1356-181109- 064939-827-947; MicrosoftAccess 2016, NumberLicense: 69201333 OPEN 99384269ZZE1912 (коммерческая лицензия, иностранный производитель); JoyClass, Договор №36/15-Л от 26.10.2015 г. СППР "Выбор", Договор № 10 от 06.02.2018 г. NetBeansIDE, лицензия freeware (свободно распространяемое ПО, иностранный производитель); MicrosoftVisualStudio 2017 CE (C#, C++), лицензия freeware (свободно распространяемое ПО, иностранный производитель); MicrosoftVisualStudio 2010 Express, лицензия freeware (свободно распространяемое ПО, иностранный производитель); MicrosoftVisualStudioCommunity, лицензия freeware (свободно распространяемое ПО, иностранный производитель); MicrosoftSQL 2010 Express, лицензия freeware (свободно распространяемое ПО, иностранный производитель); Notepad ++, лицензия freeware (свободно распространяемое ПО, иностранный производитель); MySQL, лицензия freeware (свободно распространяемое ПО, иностранный производитель); OracleSQLDeveloper, лицензия freeware; MicrosoftSOAPToolkit, лицензия freeware (свободно распространяемое ПО, иностранный производитель); CADE, лицензия freeware (свободно распространяемое ПО, иностранный производитель); Denwer 3 webserver, лицензия freeware (свободно распространяемое ПО, иностранный производитель); Dev-C++, лицензия freeware; IDEEclipse, лицензия freeware (свободно распространяемое ПО, иностранный производитель); JDK 6, лицензия freeware (свободно распространяемое ПО, иностранный производитель); Freepascal, лицензия freeware (свободно распространяемое ПО, иностранный производитель); Lazarus, лицензия freeware (свободно распространяемое ПО, иностранный производитель);

	Geany, лицензия freeware (свободно распространяемое ПО, иностранный производитель); JavaDevelopmentKit, лицензия freeware (свободно распространяемое ПО, иностранный производитель); TheRProject, лицензия freeware 9 (свободно распространяемое ПО, иностранный производитель); NetBeansIDE8, лицензия freeware (свободно распространяемое ПО, иностранный производитель); StarUML 5.0.2, лицензия freeware (свободно распространяемое ПО, иностранный производитель); EViews 9 StudentVersionLite, лицензия freeware (свободно распространяемое ПО, иностранный производитель); Gretl, лицензия freeware (свободно распространяемое ПО, иностранный производитель); Matrixer, лицензия freeware (свободно распространяемое ПО, иностранный производитель); Maxima, лицензия freeware (свободно распространяемое ПО, иностранный производитель); Xmind, лицензия freeware (свободно распространяемое ПО, иностранный производитель); BPWIN, лицензия freeware; Gimp, лицензия freeware (свободно распространяемое ПО, иностранный производитель); IrfanView, лицензия freeware (свободно распространяемое ПО, иностранный производитель); SMARTBoard, Акт №ДС – 0001621 от 06.12.12 г., Акт №ДС – 0001620 от 06.12.12 г.; 2GIS, лицензия freeware (свободно распространяемое ПО, отечественный производитель). Обеспечен доступ к сети Интернет и в электронную информационно- образовательную среду организации.
Лаборатория иностранных языков и информационных дисциплин № 403. для проведения занятий семинарского типа (практических занятий и лабораторных работ), групповых консультаций, индивидуальных консультаций, текущего контроля, промежуточной аттестации, государственной итоговой аттестации, научно- исследовательской работы обучающихся, курсового проектирования (выполнения курсовых работ)	Учебная мебель (10 столов, 18 стульев). Персональные компьютеры для работы в электронной образовательной среде с выходом в Интернет - 10 шт. Лингафонное оборудование (компьютер, мониторы 2 шт., наушники с микрофоном 10 шт.). Лицензионное программное обеспечение (NetClass). Учебно-наглядные пособия. Тематические иллюстрации. Программное обеспечение: Microsoft Windows XP Professional Russian, Number License: 43817654 OPEN 63807614ZZE1004 (коммерческая лицензия, иностранный производитель); Microsoft Office 2007 Standart Win32 Russian, Number License 42024141 OPEN 61960499ZZE0903 (коммерческая лицензия, иностранный производитель); Consultant Plus - Договор 11/01-09 от 01.09.2009 г. Доп.соглашение №1 (автопролонгация) (коммерческая лицензия, отечественный производитель ПО); Adobe Acrobat Reader, лицензия freeware (свободно распространяемое ПО, иностранный производитель); Kaspersky Endpoint Security - Russian Edition, лицензия № 1356-181109- 064939-827-947 (коммерческая лицензия, отечественный производитель ПО); CorelDRAW Graphics Suite X4, Order 3056570 15.04.2008 (коммерческая лицензия, иностранный производитель);

	NetClass PRO, Акт № ДС-0000349 от 12.02.13 г. NetBeans IDE, лицензия freeware (свободно распространяемое ПО, иностранный производитель); Microsoft Visual Studio 2017 CE (C#, C++), лицензия freeware (свободно распространяемое ПО, иностранный производитель); Microsoft Visual Studio 2010 Express, лицензия freeware (свободно распространяемое ПО, иностранный производитель); Microsoft Visual Studio Community, лицензия freeware (свободно распространяемое ПО, иностранный производитель); Microsoft SQL 2010 Express, лицензия freeware (свободно распространяемое ПО, иностранный производитель); Notepad ++, лицензия freeware (свободно распространяемое ПО, иностранный производитель); MySQL, лицензия freeware (свободно распространяемое ПО, иностранный производитель); Oracle SQL Developer, лицензия freeware (свободно распространяемое ПО, иностранный производитель); Microsoft SOAP Toolkit, лицензия freeware (свободно распространяемое ПО, иностранный производитель); CADE, лицензия freeware (свободно распространяемое ПО, иностранный производитель); Denwer 3 web server, лицензия freeware (свободно распространяемое ПО, иностранный производитель); Dev-C++, лицензия freeware (свободно распространяемое ПО, иностранный производитель); IDE Eclipse, лицензия freeware (свободно распространяемое ПО, иностранный производитель); JDK 6, лицензия freeware (свободно распространяемое ПО, иностранный производитель); Freepascal, лицензия freeware (свободно распространяемое ПО, иностранный производитель); Lazarus, лицензия freeware (свободно распространяемое ПО, иностранный производитель); Geany, лицензия freeware (свободно распространяемое ПО, иностранный производитель); Java Development Kit, лицензия freeware (свободно распространяемое ПО, иностранный производитель); The R Project, лицензия freeware (свободно распространяемое ПО, иностранный производитель); NetBeans IDE8, лицензия freeware (свободно распространяемое ПО, иностранный производитель); StarUML 5.0.2, лицензия freeware (свободно распространяемое ПО, иностранный производитель); EViews 9 Student Version Lite, лицензия freeware (свободно распространяемое ПО, иностранный производитель); Gretl, лицензия freeware (свободно распространяемое ПО, иностранный производитель); Matrixer, лицензия freeware (свободно распространяемое ПО, иностранный производитель); Maxima, лицензия freeware; Xmind, лицензия freeware (свободно распространяемое ПО, иностранный производитель); BPWIN, лицензия freeware (свободно распространяемое ПО, иностранный производитель); Gimp, лицензия freeware (свободно распространяемое

	ПО, иностранный производитель); IrfanView, лицензия freeware (свободно распространяемое ПО, иностранный производитель); 2GIS, лицензия freeware (свободно распространяемое ПО, отечественный производитель). Обеспечен доступ к сети Интернет и в электронную информационно-образовательную среду организации.
Лаборатория математических и информационных дисциплин № 416. для проведения занятий семинарского типа (практических занятий и лабораторных работ), групповых консультаций, индивидуальных консультаций, текущего контроля, промежуточной аттестации, государственной итоговой аттестации, научно- исследовательской работы обучающихся, курсового проектирования (выполнения курсовых работ)	Учебная мебель (11 столов, 22 стула, доска информационная - 2 шт., шкаф, стол и стул преподавателя). Персональные компьютеры для работы в электронной образовательной среде с выходом в Интернет - 10 шт. Лицензионное программное обеспечение, используемое в учебном процессе. Учебно- наглядные пособия. Тематические иллюстрации. Программное обеспечение: AstraLinux Special Edition РУСБ.10015-01, Лицензионный договор АО «НПО РусБИТех» № РБТ-14/1688-01-ВУЗ (коммерческая лицензия, отечественный производитель ПО); Consultant Plus - Договор 11/01-09 от 01.09.2009 г. Доп.соглашение №1 (автопролонгация) (коммерческая лицензия, отечественный производитель ПО); OpenOffice 4.1.1, лицензия freeware (свободно распространяемое ПО, иностранный производитель); LibreOffice, лицензия freeware (свободно распространяемое ПО, иностранный производитель); 2GIS, лицензия freeware (свободно распространяемое ПО, отечественный производитель). Обеспечен доступ к сети Интернет и в электронную информационно-образовательную среду организации.
Мультимедийная учебная аудитория № 422. для проведения занятий лекционного типа, занятий семинарского типа (практических занятий), групповых консультаций, индивидуальных консультаций, текущего контроля, промежуточной аттестации, государственной итоговой аттестации	Учебная мебель (18 столов, 36 стульев, доска маркерная, трибуна, шкаф, стол и стул преподавателя). Мультимедийное демонстрационное оборудование (интерактивная доска, компьютер с выходом в интернет, 2 аудиоколонки). Программное обеспечение: Microsoft Windows 8 Professional Russian, Number License: 61555010 OPEN 91563139ZZE1502 (коммерческая лицензия, иностранный производитель); Microsoft Office Standart 2007 Win32 Russian, Number License 42024141 OPEN 61960499ZZE0903 (коммерческая лицензия, иностранный производитель); Consultant Plus - Договор 11/01 -09 от 01.09.2009 г. Доп.соглашение №1 (автопролонгация) (коммерческая лицензия, отечественный производитель ПО); Adobe Acrobat Reader, лицензия freeware (свободно распространяемое ПО, иностранный производитель); Kaspersky Endpoint Security - Russian Edition, лицензия № 1356-181109- 064939-827-947; 2GIS, лицензия freeware (свободно распространяемое ПО, отечественный производитель). Обеспечен доступ к сети Интернет и в электронную информационно-образовательную среду организации.

Аудитория для самостоятельной работы студентов № 413. библиотека (читальный зал), помещение для самостоятельной работы обучающихся, научно-исследовательской работы обучающихся, курсового проектирования (выполнения курсовых работ)	Учебная мебель (9 столов, 23 стула, мягкая зона). Персональные компьютеры с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Института - 6 шт. Программное обеспечение: Microsoft Windows 8.1 Pro Russian, Number License: 63726920 OPEN 91563139ZZE1502 (коммерческая лицензия, иностранный производитель); Microsoft Windows 10 Pro Number License 67568455 OPEN 97574928ZZE1810 (коммерческая лицензия, иностранный производитель); Microsoft Office 2007 standart Win32 Russian, Number License 42024141 OPEN 61960499ZZE0903 (коммерческая лицензия, иностранный производитель); Microsoft Office Standart 2019 Number License 67568455 OPEN 97574928ZZE1810 (коммерческая лицензия, иностранный производитель); Consultant Plus (коммерческая лицензия, отечественный производитель); Adobe Acrobat Reader (свободно распространяемое ПО, иностранный производитель); Kaspersky Endpoint Security - Russian Edition, лицензия № 1356¬181109¬064939¬827¬947 (коммерческая лицензия, отечественный производитель); 2GIS (свободно распространяемое ПО, отечественный производитель). Обеспечен доступ к сети Интернет и в электронную информационно-образовательную среду организации.
Аудитория № 420. помещение для хранения и профилактического обслуживания учебного оборудования - компьютерного оборудования и хранения элементов мультимедийных лабораторий	Мебель (4 стола, 4 стула, стеллажи), 4 персональных компьютера для системного администратора, ведущего специалиста информационного отдела, инженера-электронщика, 10 серверов. Паяльная станция, стеллаж, 15 планшетных компьютеров, наушники для лингафонного кабинета, запасные части для компьютерного оборудования.
Аудитория № 003. помещение для хранения и профилактического обслуживания учебного оборудования	Станок для сверления, угловая шлифовальная машина, наборы слесарных инструментов для обслуживания учебного оборудования, запасные части для столов и стульев. Стеллаж, материалы для сопровождения учебного процесса.

Для проведения учебных занятий по дисциплине используются следующие комплекты лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:

Наименование	Основание	Описание
Microsoft Office Professional Plus 2013	Open License 62668528	Пакет электронных редакторов
Microsoft Office Standard 2016	Open License 66020759	Пакет электронных редакторов
Microsoft Office Standard 2007	Open License 42024141	Пакет электронных редакторов
OpenOffice 4.1.1	Freeware	Пакет электронных редакторов

LibreOffice	Freeware	Пакет электронных редакторов
JoyClass	Договор №36/15-Л от 26.10.2015 г.	Лингафонный кабинет
NetClass PRO	Акт № ДС-0000349 от 12.02.13 г.	Лингафонный кабинет
Adobe Acrobat Reader	Freeware	Пакет программ для создания и просмотра электронных публикаций в формате PDF
CADE	Freeware	CAD-программа для проектирования схем, из-делий, деталей, предметов, конструкций
Consultant Plus	Доп.соглашение №1 к договору № 11/01-09 от 01.09.2009	ЭСС Консультант+
Microsoft Office Standard 2013	Open License 637269920	Пакет электронных редакторов
Notepad ++	Freeware	Пакет электронных редакторов
Microsoft Visual Studio 2017 CE (C#, C++)	Подписка на 3 года	Интегрированная среда разработки приложе-ний, ПО
Dev-C++	Freeware	Приложение по программированию
Geany	Freeware	среда разработки программного обеспечения
Lazarus	Freeware	компилятор языка программирования Pascal
Microsoft Visual Studio Community	Freeware для академических учреждений	Интегрированная среда разработки для создания современных приложений Android, IOS и Windows, а также веб- приложений и облачных служб

12. СРЕДСТВА АДАПТАЦИИ ПРЕПОДАВАНИЯ ДИСЦИПЛИНЫ К ПОТРЕБНОСТЯМ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья и инвалидов (по заявлению обучающегося) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических особенностей, в том числе с применением электронного обучения и дистанционных технологий:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации.
- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.
- для лиц с нарушениями опорнодвигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями. Эти средства могут быть предоставлены вузом или могут использоваться собственные технические средства. Проведение процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья допускается с использованием дистанционных образовательных технологий.

При необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на выполнение заданий текущего контроля. Процедура проведения промежуточной аттестации для обучающихся с ограниченными возможностями здоровья и обучающихся инвалидов устанавливается с учётом индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

Приложение 1

Технологическая карта дисциплины

Наименование дисциплины	Информационная безопасность ИС
Количество зачетных единиц	3
Форма промежуточной аттестации	Зачет

№	Виды учебной деятельности студентов	Форма отчетности	Баллы (максимум)
Текущий контроль			
1	Посещение и работа на лекционных и практических занятиях (собеседование, контрольная работа, круглый стол и дискуссия)		
2	Выполнение письменного задания (реферат)	Письменная работа	
3	Выполнение практического задания (кейс)	Письменная работа	
Промежуточная аттестация			
4	Выполнение итоговой работы	Итоговая работа, тест	
		Итого по дисциплине:	100

«____» _____ 20___ г.

Преподаватель _____ / _____

(уч. степень, уч. звание, должность, ФИО преподавателя) Подпись

Приложение 2

Номер темы для выполнения реферата

Буква фамилии	а	б	в	г	д	е	ж	з	и	к	л	м	н	о
Номер темы реферата	1 или 15	2 или 16	3 или 17	4 или 18	5 или 19	6 или 20	7 или 14	8 или 13	9 или 12	10 или 1	11 или 2	12 или 3	13 или 4	14 или 5
Буква фамилии	п	р	с	т	у	ф	х	ц	ч	ш	щ	э	ю	я
Номер темы реферата	15 или 6	16 или 7	17 или 8	18 или 9	19 или 10	20 или 4	21 или 5	22 или 6	23 или 7	24 или 8	25 или 7	6 или 23	7 или 24	8 или 25

Приложение 3

Исходные данные расчетно-графического задания

Примечание. подробное описание оценки опасности угроз и построения модели нарушителя ИБ приведено в книге: **Моргунов, А. В. Информационная безопасность: учебно-методическое пособие**: / А. В. Моргунов; Новосибирский государственный технический университет. – Новосибирск: Новосибирский государственный технический университет, 2019. – 83 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=576726

Варианты задания

Первая буква фамилии студента	Вариант
А	1
Б	2
В	3
Г	4
Д	5
Е, Ё	1
Ж, З	2
И, К	3
Л	4
М	5
Н	1
О	2
П	3
Р	4
С	5
Т	1
У, Ф	2
Х, Ц, Ч	3
Ш, Щ	4
Э, Ю, Я	5

Вариант 1

Исходные данные: организация, имеющая три автоматизированные системы: ИСПДн первого класса, ИСПДн второго класса и ИС конфиденциальной информации. Режимы обработки – многопользовательские с различными правами доступа. Все системы являются локальными, однако расположены в двух зданиях в разных концах города. Выход в сеть Интернет осуществляется через единый коммутационный узел в здании № 1; здания № 1 и 2 объединены ВОЛС (рис. П1).

Среди сотрудников присутствуют следующие категории пользователей: пользователи ИС, системные администраторы, администраторы безопасности, разработчики прикладного ПО. Информационные системы после обработки предоставляют сторонним пользователям информацию в рамках существующего законодательства.

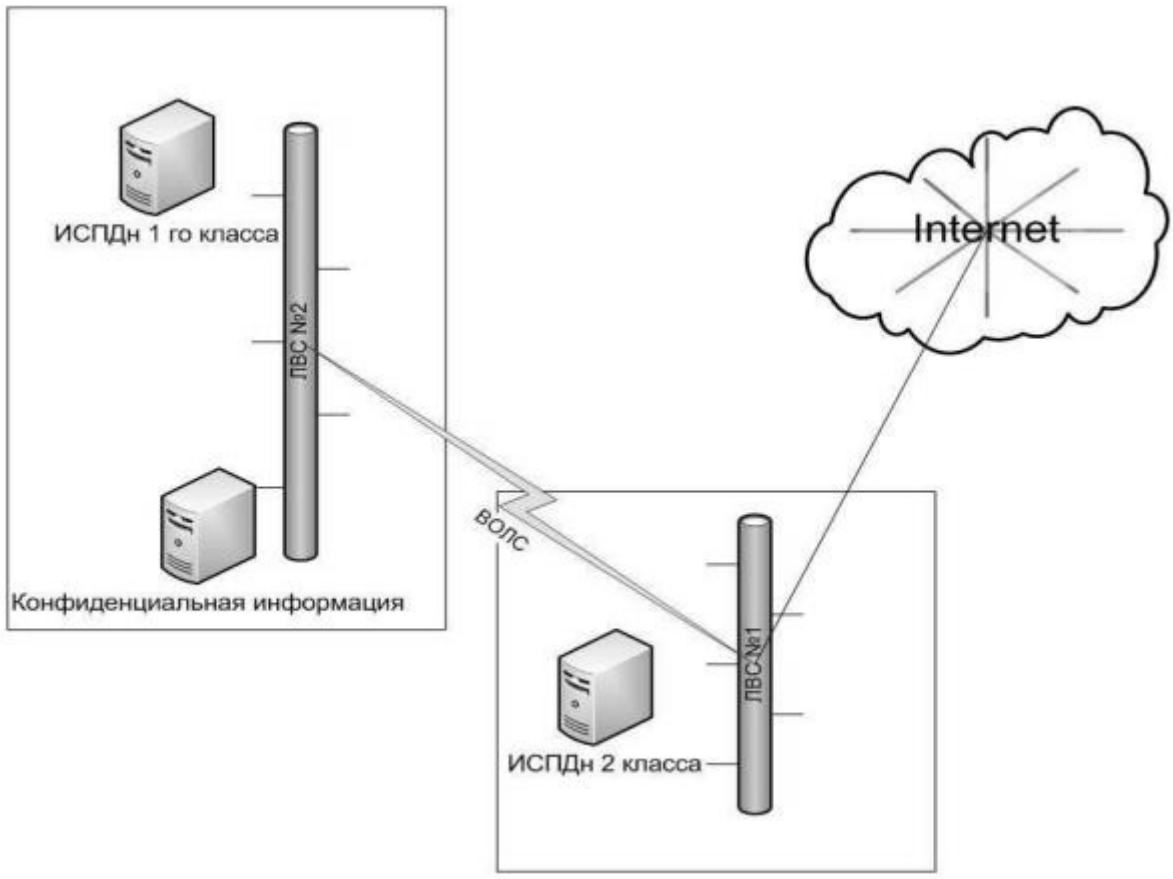

Рис. П1. Исходная схема для варианта 1

Вариант 2

Исходные данные: организация, имеющая две автоматизированные системы: ИСПДн первого класса, ИСПДн второго класса. Режимы обработки – многопользовательские. Все системы являются распределенными и расположены в трех зданиях в разных концах города. Выход в сеть Интернет осуществляется в каждом из трех зданий (рис. П2).

Среди сотрудников присутствуют следующие категории пользователей: пользователи ИС, системные администраторы, администраторы безопасности. Информационные системы после обработки предоставляют сторонним пользователям информацию в рамках существующего законодательства.

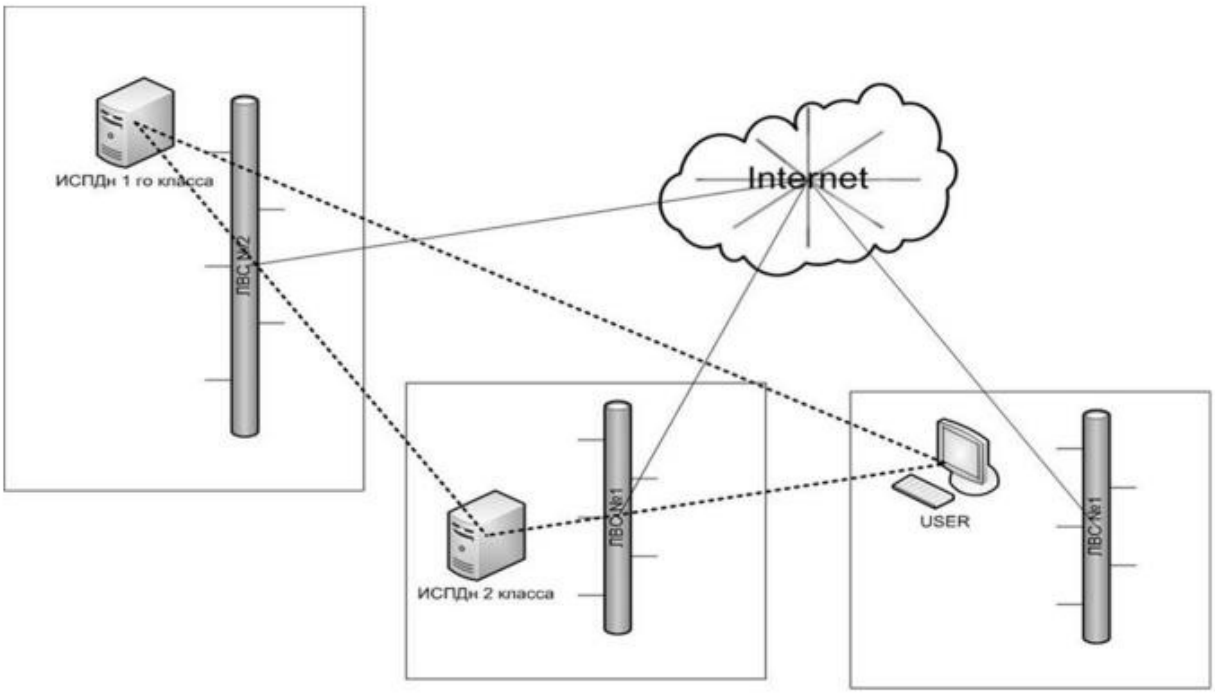

Рис. П2. Исходная схема для варианта 2

Вариант 3

Исходные данные: организация, имеющая три автоматизированные системы: ИСПДн первого класса, ИСПДн второго класса и ИС конфиденциальной информации. Режимы обработки – многопользовательские с различными правами доступа. Все системы являются распределенными и расположены в двух корпусах рядом стоящих помещений, обладающих общей территорией. Выход в сеть Интернет осуществляется через единый коммутационный узел в здании № 1; здания № 1 и 2 объединены ВОЛС (рис. П3).

Среди сотрудников присутствуют следующие категории пользователей: пользователи ИС, системные администраторы. Информационные системы после обработки не предоставляют сторонним пользователям никакой информации.

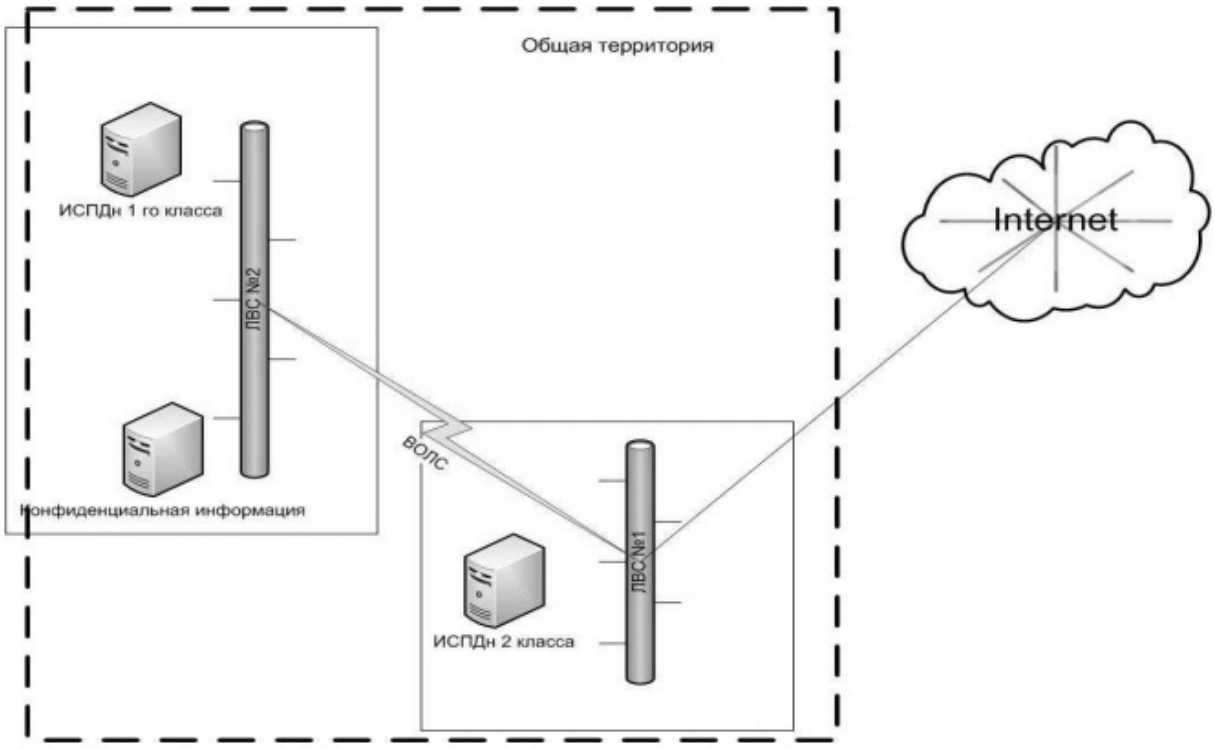

Рис. П3. Исходная схема к варианту 3

Вариант 4

Исходные данные: организация, имеющая две автоматизированные системы: ИСПДн второго класса и ИС конфиденциальной информации. Режимы обработки – однопользовательские. Все системы являются автономными, однако в рамках оказания услуг производится передача данных контрагентам. Выход в сеть Интернет осуществляется через два канала связи (рис. П4). Среди сотрудников присутствуют следующие категории пользователей: пользователи ИС, системные администраторы, администраторы безопасности, разработчики прикладного ПО. Информационные системы после обработки предоставляют сторонним пользователям информацию в рамках существующего законодательства.

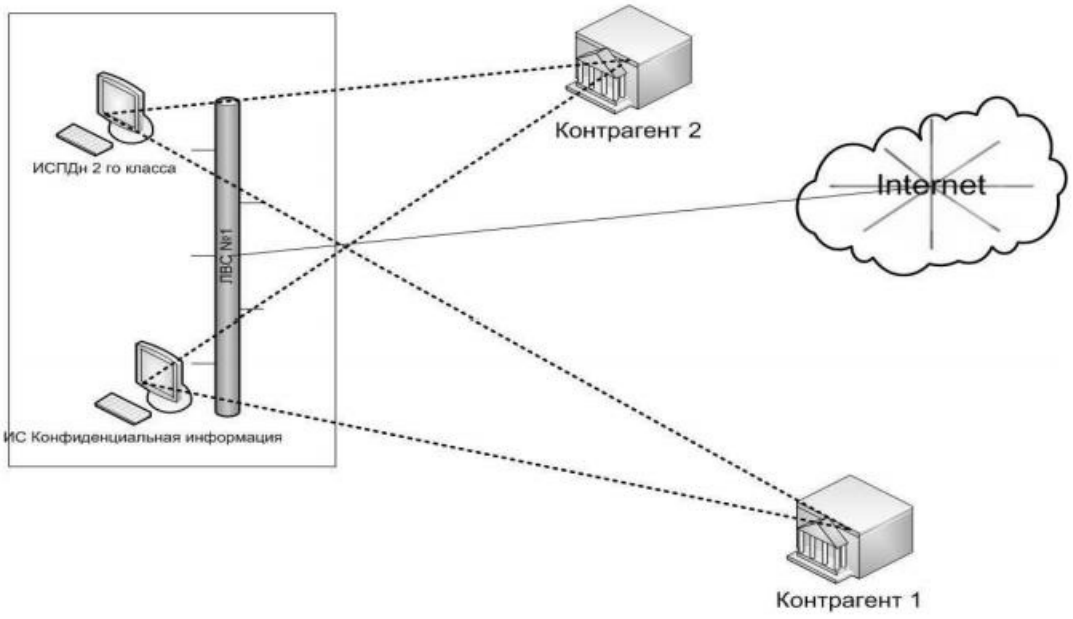

Рис. П4. Исходная схема к варианту

Вариант 5

Исходные данные: организация, имеющая три автоматизированные системы: ИСПДн первого класса, ИС конфиденциальной информации 1 и ИС конфиденциальной информации 2. Режимы обработки ИСПДн и ИС конфиденциальной информации 1 многопользователь- 69 ские с различными правами доступа, ИС конфиденциальной информации 2 – многопользовательская. Все системы являются распределенными и расположены в двух зданиях в разных концах города. Выход в сеть Интернет осуществляется через единый коммутационный узел в здании № 1, здания № 1 и 2 объединены ВОЛС (рис. П5).

Среди сотрудников присутствуют следующие категории пользователей: пользователи ИС, системные администраторы, администраторы безопасности, разработчики прикладного ПО. Информационные системы после обработки предоставляют сторонним пользователям информацию в рамках существующего законодательства.

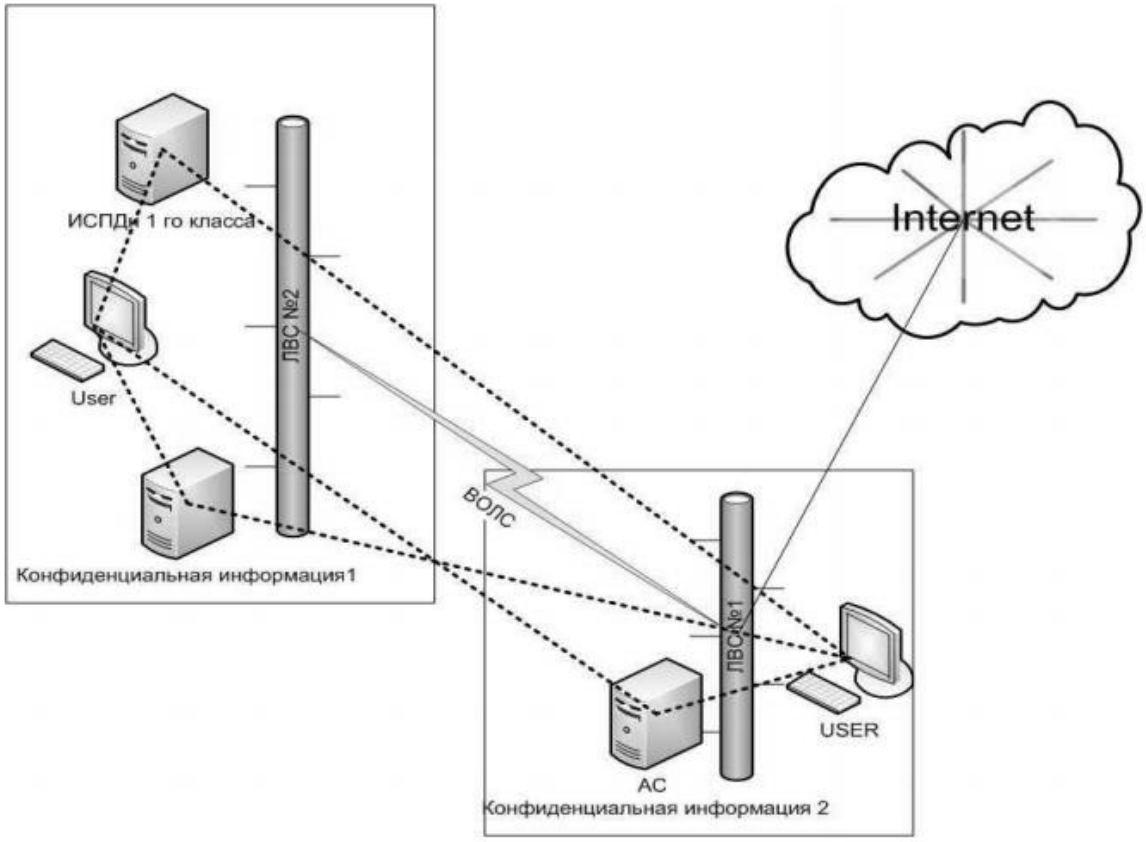

Рис. П5. Исходная схема к варианту 5

Приложение 4

Итоговый тест

1. Свойство информации не иметь скрытых ошибок – это:

1. полнота
2. ценность
3. достоверность
4. новизна, актуальность

2. Свойство информации, отражающее невозможность несанкционированного использования – это:

1. своевременность
2. ценность
3. достоверность
4. защищенность

3. Основной документ, на основе которого проводится политика информационной безопасности – это

1. программа информационной безопасности
2. регламент информационной безопасности
3. политическая информационная безопасность
4. Протекторат

4. Свойство информации - приведение данных, поступающих из разных источников, к одинаковой форме, что позволяет сделать их сопоставимыми между собой, - это

1. Формализация данных
2. Фильтрация данных
3. Архивация данных
4. Защита данных

5. Комплекс мер, направленных на предотвращение потерь, воспроизведения и модификации данных – это информационный процесс:

1. Формализации данных
2. Фильтрации данных
3. Архивации данных
4. Защиты данных

6. Из следующих утверждений выберите одно неверное:

1. Термин «компьютерная безопасность» можно употреблять как заменитель термина «информационная безопасность»
2. Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности
3. Информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации

7. Составляющими информационной безопасности являются:

1. обеспечение доступности, целостности
2. обеспечение доступности, конфиденциальности информационных ресурсов и поддерживающей инфраструктуры
3. обеспечение целостности, конфиденциальности информационных ресурсов и поддерживающей инфраструктуры
4. обеспечение доступности, целостности, конфиденциальности информационных ресурсов и поддерживающей инфраструктуры

8. Возможность за приемлемое время получить требуемую информационную услугу – это составляющая информационной безопасности:

1. Доступность
2. Целостность

3. Конфиденциальность

9. Актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения – это составляющая информационной безопасности:

1. Доступность
2. Целостность
3. Конфиденциальность

10. Первым и наиболее известным документом по стандартизации в области информационной безопасности является:

1. Британский стандарт BS 7799
2. Оранжевая книга (1985 г.)
3. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения.

11. Защита от несанкционированного доступа к информации – это составляющая информационной безопасности:

1. Доступность
2. Целостность
3. Конфиденциальность

12. Потенциальная возможность определенным образом нарушить информационную безопасность – это:

1. взлом
2. угроза
3. хакерская атака
4. кража информации

13. Попытка реализации угрозы называется:

1. несанкционированным доступом
2. атакой
3. уязвимостью
4. кражей

14. По аспекту информационной безопасности выделяют угрозы:

1. доступности, целостности, конфиденциальности
2. случайные/преднамеренные, действия природного/техногенного характера
3. внутри/вне рассматриваемой ИС
4. данных, программ, аппаратуры, поддерживающей инфраструктуры

15. Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, называется:

1. угрозой
2. окном опасности
3. атакой
4. взломом

16. По расположению источника угроз выделяют угрозы:

1. доступности, целостности, конфиденциальности
2. случайные/преднамеренные, действия природного/техногенного характера
3. внутри/вне рассматриваемой ИС
4. данных, программ, аппаратуры, поддерживающей инфраструктуры

17. Из следующих утверждений выберите одно неверное:

1. Пока существует окно опасности, возможны успешные атаки на ИС.
2. Потенциальные злоумышленники называются источниками угрозы.
3. Чаще всего угроза является следствием наличия уязвимых мест в защите информационных систем.
4. Пока существует окно опасности, не возможны атаки на ИС.

18. По способу осуществления выделяют угрозы:

1. доступности, целостности, конфиденциальности
2. случайные/преднамеренные, действия природного/техногенного характера
3. внутри/вне рассматриваемой ИС
4. данных, программ, аппаратуры, поддерживающей инфраструктуры

19. По компонентам информационных систем, на которые угрозы нацелены, выделяют угрозы:

1. доступности, целостности, конфиденциальности
2. случайные/преднамеренные, действия природного/техногенного характера
3. внутри/вне рассматриваемой ИС
4. данных, программ, аппаратуры, поддерживающей инфраструктуры

20. Ввод неверных данных, нарушение атомарности транзакций, переупорядочение, дублирование данных относятся к угрозам:

1. доступности
2. целостности
3. конфиденциальности

21. К основным видам защищаемой информации, оборот которой контролируется, относятся:

1. объекты промышленной собственности, объекты авторского права
2. служебная тайна, государственная тайна, объекты интеллектуальной собственности
3. профессиональная тайна, персональные данные

22. К основным видам защищаемой информации – государственных секретов, относятся:

1. объекты промышленной собственности, объекты авторского права
2. служебная тайна, государственная тайна.
3. профессиональная тайна, персональные данные

23. Основным содержанием кадровой информации являются:

1. Карты и журналы ИТ-инфраструктуры, ИТ-системы, системы доступа
2. Личные карточки персонала
3. Регистрационные и уставные документы, нормативы
4. Файлы и документы для внутреннего обмена данными

24. Основным содержанием внутрикорпоративной информации являются:

1. Приказы, распоряжения, расписания, отчеты собраний проектных групп, документы системы качества
2. Регистрационные и уставные документы, нормативы
3. Файлы и документы для внутреннего обмена данными
4. Фотографии, видеоролики, фильмы, аудиокниги

25. Дешифрование –:

1. процесс применения шифра к защищаемой информации
2. преобразование исходного сообщения в зашифрованное
3. преобразование шифрованного сообщения в исходное

26. По особенностям алгоритма шифрования выделяют криптосистемы:

1. совершенные, практически стойкие, стойкие
2. симметричные, асимметричные, квантовые, комбинированные
3. потоковые, блочные

27. Шифрование с помощью таблицы Вижинера относится к:

1. симметричным криптосистемам
2. асимметричным криптосистемам
3. квантовой криптографии
4. комбинированным (составным) методам

28. По количеству символов сообщения выделяют криптосистемы:

1. совершенные, практически стойкие, стойкие
2. симметричные, асимметричные, квантовые, комбинированные

3. потоковые, блочные

29. Шифрование с помощью моноалфавитной подстановки относится к:

1. симметричным криптосистемам
2. асимметричным криптосистемам
3. квантовой криптографии
4. комбинированным (составным) методам

30. По стойкости шифра выделяют криптосистемы:

1. совершенные, практически стойкие, стойкие
2. симметричные, асимметричные, квантовые, комбинированные
3. потоковые, блочные

31. Шифрование методом перестановки относится к:

1. симметричным криптосистемам
2. асимметричным криптосистемам
3. квантовой криптографии
4. комбинированным (составным) методам

32. Определите метод шифрования исходного сообщения:

Исходное сообщения: безопасность

Результат шифрования: ьтсо нсап озеб

1. усложненная перестановка по таблице
2. усложненная перестановка по маршрутам
3. простая перестановка

33. Исходное сообщение: пара**. Зашифрованное сообщение:** свтв**. Частоты появления символов в зашифрованном сообщении равны:**

1. с – 0.4, в – 0.6, т – 0.2.
2. с – 0.25, в – 0.5, т – 0.25.
3. с – 0.4, в – 0.6, т – 0.4.
4. с – 0.1, в – 0.2, т – 0.1.

34. Набор правил (инструкций), определяющих содержание и порядок операций по шифрованию и дешифрованию информации, называется:

1. криптографической системой
2. алгоритмом криптографического преобразования
3. криптоанализом
4. криптографией

35. Практическое применение аутентификации на основе опознавания в диалоговом режиме выполняется:

1. при входе в систему на основе сравнения пароля с эталоном
2. на основе персонифицирующих данных пользователя или достаточно большого и упорядоченного набора паролей
3. на основе индивидуальных особенностей и физиологических характеристик пользователя

36. Разграничение доступа к элементам защищаемой информации по кольцам секретности предполагает:

1. составление для каждого элемента защищаемых данных списка всех тех пользователей, которым предоставлено право доступа к соответствующему элементу
2. распределение защищаемых данных по массивам таким образом, чтобы в каждом массиве содержались данные одного уровня секретности
3. формирование двумерной таблицы, по строкам которой расположены идентификаторы зарегистрированных пользователей, а по столбцам – идентификаторы защищаемых элементов данных

37. Процедура распознавания субъекта по его имени называется:

1. аутентификацией

2. идентификацией
3. авторизацией

38. Практическое применение аутентификации на основе распознавания по простому паролю выполняется:

1. при входе в систему на основе сравнения пароля с эталоном
2. на основе персонифицирующих данных пользователя или достаточно большого и упорядоченного набора паролей
3. на основе индивидуальных особенностей и физиологических характеристик пользователя

39. Способ разового разрешения на допуск к защищаемому элементу данных – это разграничение доступа к элементам защищаемой информации по:

1. по матрицам полномочий
2. кольцам секретности
3. по мандатам
4. по специальным спискам

40. Процедура проверки подлинности называется:

1. аутентификацией
2. идентификацией
3. авторизацией

41. Процедура входа пользователя в систему путем задания имени и пароля является примером:

1. аутентификации
2. идентификации
3. авторизации

42. Программное обеспечение или оборудование, которое позволяет проверять данные, получаемые через Интернет или сеть, и блокировать их или пропускать на компьютер называется:

1. антивирусным комплексом
2. брандмауэром
3. роутером
4. шлюзом

43. Процедура предоставления субъекту определённых прав называется:

1. аутентификацией
2. идентификацией
3. авторизацией

44. Под угрозой удаленного администрирования в компьютерной сети понимается угроза:

1. несанкционированного управления удаленным компьютером
2. внедрения агрессивного программного кода в рамках активных объектов Web-страниц
3. перехвата или подмены данных на путях транспортировки
4. вмешательства в личную жизнь
5. поставки неприемлемого содержания

45. Основные предметные направления защиты информации:

1. Охрана государственной, коммерческой, служебной, банковской тайн, персональных данных и интеллектуальной собственности
2. Охрана золотого фонда страны
3. Определение ценности информации
4. Усовершенствование скорости передачи информации

46. Элемент аппаратной защиты ИС, где используется установка источников бесперебойного питания (UPS) – это

1. защита от сбоев в электропитании

2. защита от сбоев серверов, рабочих станций и локальных компьютеров
3. защита от сбоев устройств для хранения информации
4. защита от утечек информации электромагнитных излучений

47. Элемент аппаратной защиты, где используется резервирование особо важных компьютерных подсистем

1. защита от сбоев в электропитании
2. защита от сбоев серверов, рабочих станций и локальных компьютеров
3. защита от сбоев устройств для хранения информации
4. защита от утечек информации электромагнитных излучений

48. Учет всех возможных коммуникационных каналов, обеспечения физической безопасности, шифрования резервных копий и информации, покидающей корпоративный периметр, и других организационных мероприятий - это

1. Индивидуальный подход к защите
2. Комплексный подход к защите
3. Смешанный подход к защите
4. Рациональный подход к защите

49. Защита от сбоев серверов, рабочих станций и локальных компьютеров относится к

1. Аппаратным и техническим средствам защиты
2. Программным средствам защиты
3. Средствам защиты идентификации и аутентификации
4. Организационным и общим средствам защиты

50. Развитие современных средств безбумажного документооборота, средств электронных платежей немыслимо без развития средств доказательства подлинности и целостности документа. Таким средством является

1. электронно-цифровая подпись
2. протокол секретности
3. аутентификация
4. биометрия
5. идентификация пользователя
6. водяные знаки

Приложение 5.

Варианты для выполнения итоговой работы

Первая буква фамилии студента	№ заданий
А, Б	1
В, Г	2
Д, Е, Ё	3
Ж, З	4
И, К	1
Л, М	2
Н, О	3
П , Р	4
С	1
Т	2
У, Ф	3
Х, Ц, Ч	4
Ш, Щ	1
Э, Ю, Я	2

Лист регистрации изменений, дополнений и ревизий документа

№ п/п	Дата внесения изменения	Документ, на основании которого внесено	Краткое содержание изменения
1	2	3	4
1	01.09.2021 г.	Протокол решения УС № 1 от 01.09.2021 г.	Внесение изменений в федеральные государственные образовательные стандарты высшего образования (Приказ Министерства науки и высшего образования Российской Федерации от 26 ноября 2020 г. № 1456)
2	26.01.2022 г.	Протокол решения УС № 6 от 26.01.2022 г.	1. Актуализация комплектов оценочных материалов для проведения промежуточной аттестации обучающихся по дисциплине; 2. Актуализация перечня основной и дополнительной учебной литературы, необходимой для освоения дисциплины; 3. Актуализация перечня ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины; 4. Актуализация методических указаний для обучающихся по освоению дисциплины; 5. Актуализация перечня современных профессиональных баз данных и информационных справочных систем; 6. Актуализация материально-технического и программного обеспечения, необходимого для осуществления образовательного процесса по дисциплине.