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

УТВЕРЖДЕНО:
Ректор
Родионов М. Г.
(протокол от 28.08.2024 № 12)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ) «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ИС»

Уровень высшего образования: бакалавриат

Направление подготовки: 09.03.03 Прикладная информатика

Направленность (профиль)подготовки: Прикладная информатика в экономике

Квалификация (степень) выпускника: бакалавр

Формы обучения: очная, очно-заочная, заочная

Год набора (приема на обучение): 2024

Срок получения образования: Очная форма обучения – 4 года
Очно-заочная форма обучения – 4 года 10 месяца(-ев)
Заочная форма обучения – 4 года 10 месяца(-ев)

Объем: в зачетных единицах: 3 з.е.
в академических часах: 108 ак.ч.

г. Омск, 2024

Разработчики:
Старший преподаватель, факультет очного обучения
Куликова Е. В.

Рецензенты:
Ультан А.Е., доцент кафедры «Информационная безопасность» Омского государственного университета путей сообщения, к.т.н.

Рабочая программа дисциплины (модуля) составлена в соответствии с требованиями ФГОС ВО по направлению подготовки Направление подготовки: 09.03.03 Прикладная информатика, утвержденного приказом Минобрнауки России от 19.09.2017 №922, с учетом трудовых функций профессиональных стандартов: "Программист", утвержден приказом Минтруда России от 20.07.2022 № 424н; "Специалист по информационным системам", утвержден приказом Минтруда России от 13.07.2023 № 586н; "Руководитель проектов в области информационных технологий", утвержден приказом Минтруда России от 27.04.2023 № 369н; "Системный аналитик", утвержден приказом Минтруда России от 27.04.2023 № 367н.

Согласование и утверждение

№	Подразделение или коллегиальный орган	Ответственное лицо	ФИО	Виза	Дата, протокол (при наличии)
1		Руководитель образовательной программы	Родионов М. Г.	Согласовано	28.08.2024, № 12

Содержание (рабочая программа)

1. Цель и задачи освоения дисциплины (модуля)

Цель освоения дисциплины - 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 изучения 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.

2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Компетенции, индикаторы и результаты обучения

ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

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

Знать:

ОПК-3.1/Зн10 Основные угрозы безопасности информации и виды защищаемой информации

ОПК-3.1/Зн11 Основные требования и составляющие информационной безопасности

ОПК-3.1/Зн12 Стандарты в области информационной безопасности

ОПК-3.1/Зн13 Методы и средства обеспечения информационной безопасности компьютерных систем, механизмы защиты информации

ОПК-3.1/Зн14 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:

ОПК-3.2/Ум9 Анализировать виды угроз безопасности информации и информационных систем

ОПК-3.2/Ум10 Выбирать методы и средства обеспечения информационной безопасности компьютерных систем

ОПК-3.2/Ум11 Использовать программные, технические, организационные средства обеспечения информационной безопасности

3. Место дисциплины в структуре ОП

Дисциплина (модуль) «Информационная безопасность ИС» относится к обязательной части образовательной программы и изучается в семестре(ах): Очная форма обучения - 7, Очно-заочная форма обучения - 9, Заочная форма обучения - 9.

Предшествующие дисциплины (практики) по связям компетенций:

Информатика и информационные технологии;

Информационно-библиографическая культура;

Информационные технологии в экономике и управлении;

Ознакомительная практика;

Сети и системы передачи информации;

Технологическая (проектно-технологическая) практика;

Последующие дисциплины (практики) по связям компетенций:

Выполнение и защита выпускной квалификационной работы;

В процессе изучения дисциплины студент готовится к видам профессиональной деятельности и решению профессиональных задач, предусмотренных ФГОС ВО и образовательной программой.

4. Объем дисциплины и виды учебной работы

Очная форма обучения

Период обучения	Общая трудоемкость (часы)	Общая трудоемкость (ЗЕТ)	Контактная работа (часы, всего)	Консультации (часы)	Лабораторные занятия (часы)	Лекционные занятия (часы)	Практические занятия (часы)	Самостоятельная работа (часы)	Промежуточная аттестация (часы)
Седьмой семестр	108	3	76	4	18	36	18	23	Зачет (9)
Всего	108	3	76	4	18	36	18	23	9

Очно-заочная форма обучения

Период обучения	Общая трудоемкость (часы)	Общая трудоемкость (ЗЕТ)	Контактная работа (часы, всего)	Консультации (часы)	Лабораторные занятия (часы)	Лекционные занятия (часы)	Практические занятия (часы)	Самостоятельная работа (часы)	Промежуточная аттестация (часы)
Девятый семестр	108	3	40	4	12	12	12	64	Зачет (4)
Всего	108	3	40	4	12	12	12	64	4

Заочная форма обучения

Период обучения	Общая трудоемкость (часы)	Общая трудоемкость (ЗЕТ)	Контактная работа (часы, всего)	Консультации (часы)	Лабораторные занятия (часы)	Лекционные занятия (часы)	Практические занятия (часы)	Самостоятельная работа (часы)	Промежуточная аттестация (часы)
Девятый семестр	108	3	12	4	2	4	2	92	Зачет (4)
Всего	108	3	12	4	2	4	2	92	4

5. Содержание дисциплины

5.1. Разделы, темы дисциплины и виды занятий

(часы промежуточной аттестации не указываются)

Очная форма обучения

Наименование раздела, темы	Всего	Консультации	Лабораторные занятия	Лекционные занятия	Практические занятия	Самостоятельная работа	Планируемые результаты обучения, соотнесенные с результатами освоения программы
Раздел 1. Информационная безопасность ИС	**99**	**4**	**18**	**36**	**18**	**23**	ОПК-3.1 ОПК-3.2
Тема 1.1. Основы информационной безопасности	22			8	8	6	
Тема 1.2. Угрозы информационной безопасности	18		2	6	4	6	
Тема 1.3. Основы защиты информационных ресурсов. Построение системы информационной безопасности	12		4	4		4	
Тема 1.4. Обеспечение информационной безопасности информационных и компьютерных систем	47	4	12	18	6	7	
Итого	**99**	**4**	**18**	**36**	**18**	**23**	

Очно-заочная форма обучения

Наименование раздела, темы		ьтации	торные занятия	онные занятия	ческие занятия	оятельная работа	уемые результаты ия, соотнесенные с атами освоения ммы

	Всего	Консул	Лабора	Лекцис	Практи	Самост	Планир обучени результ програм
Раздел 1. Информационная безопасность ИС	**104**	**4**	**12**	**12**	**12**	**64**	ОПК-3.1 ОПК-3.2
Тема 1.1. Основы информационной безопасности	26		2	4	4	16	
Тема 1.2. Угрозы информационной безопасности	24		4	2	2	16	
Тема 1.3. Основы защиты информационных ресурсов. Построение системы информационной безопасности	26		4	4	2	16	
Тема 1.4. Обеспечение информационной безопасности информационных и компьютерных систем	28	4	2	2	4	16	
Итого	**104**	**4**	**12**	**12**	**12**	**64**	

Заочная форма обучения

Наименование раздела, темы	Всего	Консультации	Лабораторные занятия	Лекционные занятия	Практические занятия	Самостоятельная работа	Планируемые результаты обучения, соотнесенные с результатами освоения программы
Раздел 1. Информационная безопасность ИС	**104**	**4**	**2**	**4**	**2**	**92**	ОПК-3.1 ОПК-3.2
Тема 1.1. Основы информационной безопасности	24			2		22	
Тема 1.2. Угрозы информационной безопасности	26		2			24	
Тема 1.3. Основы защиты информационных ресурсов. Построение системы информационной безопасности	24			2		22	
Тема 1.4. Обеспечение информационной безопасности информационных и компьютерных систем	30	4			2	24	
Итого	**104**	**4**	**2**	**4**	**2**	**92**	

5.2. Содержание разделов, тем дисциплин

Раздел 1. Информационная безопасность ИС

Тема 1.1. Основы информационной безопасности

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.
2) 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.
3) 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.
4) Критерии безопасности компьютерных систем «Оранжевая книга». Руководящие документы Гостехкомиссии (ФСТЭК) России. Стандарты по управлению информационной безопасностью ISO/IEC 27000.

Тема 1.2. Угрозы информационной безопасности

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

Тема 1.3. Основы защиты информационных ресурсов. Построение системы информационной безопасности

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.

Тема 1.4. Обеспечение информационной безопасности информационных и компьютерных систем

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.
2) Классификация алгоритмов криптографических методов. Методы полиалфавитной замены. Скремблирование потока данных. Двуключевые системы шифрования. Шифрование на базе клеточных автоматов. Использование плавающего окна.
3) 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.
4) 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.
5) Механизмы контроля доступа. Средства контроля и управления доступом в ИС. Компоненты ОС для защиты информации.
6) Механизмы цифровой подписи. Однонаправленные хэш-функции. Российский стандарт хэш-функции. ГОСТ Р34.11-94. Российский стандарт цифровой подписи. ГОСТ Р 34.10 – 2001.
7) 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.

6. Рекомендуемые образовательные технологии

При преподавании дисциплины 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;
- лекции с разбором практических ситуаций.

Семинарские занятия по дисциплине 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.
Большинство практических занятий проводятся с применением активных форм обучения, к которым относятся:
1) устный опрос студентов с элементами беседы и дискуссии по вопросам, выносимым на практические занятия;
2) групповая работа студентов, предполагающая совместное обсуждение какой-либо проблемы (вопроса) и выработку единого мнения (позиции) по ней (метод группового обсуждения, круглый стол);
3) контрольная работа по отдельным вопросам, целью которой является проверка знаний

студентов и уровень подготовленности для усвоения нового материала по дисциплине.
На семинарских 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.

7. Порядок проведения промежуточной аттестации

Промежуточная аттестация: Очная форма обучения, Зачет, Седьмой семестр.
1. Работа с тестовыми заданиями
2. Выполнение итоговой работы

Промежуточная аттестация: Очно-заочная форма обучения, Зачет, Девятый семестр.
1. Работа с тестовыми заданиями
2. Выполнение итоговой работы

Промежуточная аттестация: Заочная форма обучения, Зачет, Девятый семестр.
1. Работа с тестовыми заданиями
2. Выполнение итоговой работы

8. Оценочные материалы текущего контроля

Раздел 1. Информационная безопасность ИС
Контролируемые ИДК: ОПК-3.1 ОПК-3.2

Тема 1.1. Основы информационной безопасности

Форма контроля/оценочное средство: Посещение и работа на лекционных и практических занятиях

Вопросы/Задания:

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:

Практическое занятие 1.
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.

Практическое занятие 2.
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.

Практическое занятие 3.
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 1.2. Угрозы информационной безопасности

Форма контроля/оценочное средство: Посещение и работа на лекционных и практических занятиях

Вопросы/Задания:

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:

Практическое занятие 1.
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.

Лабораторное занятие 1.
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.

Практическое занятие 2.
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 1.3. Основы защиты информационных ресурсов. Построение системы информационной безопасности

Форма контроля/оценочное средство: Посещение и работа на лекционных и практических занятиях

Вопросы/Задания:

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:

Лабораторное занятие.
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 1.4. Обеспечение информационной безопасности информационных и компьютерных систем

Форма контроля/оценочное средство: Посещение и работа на лекционных и практических занятиях

Вопросы/Задания:

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:

Практическое занятие 1.
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.

Лабораторное занятие 1.
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.

Практическое занятие 2.
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.

Практическое занятие 3.
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.

Лабораторное занятие 2.
Защита информации средствами офисных приложений.
1. Создание защищенных текстовых документов.
2. Создание защищенных электронных таблицы.
3. Создание защищенных баз данных.

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

Лабораторное занятие 4.
Однонаправленные хэш-функции. Системы шифрования с открытым ключом как основа построения систем электронной цифровой подписи.

Лабораторное занятие 5.
Выбор методов и средств обеспечения информационной безопасности компьютерной системы. Выбор сервисных программ, в частности антивирусного программного обеспечения. Настройка, обновление и использование антивирусных программ.

9. Оценочные материалы промежуточной аттестации

Очная форма обучения, Седьмой семестр, Зачет
Контролируемые ИДК: ОПК-3.1 ОПК-3.2
Вопросы/Задания:

1. Работа с тестовыми заданиями

Тестовые задания представлены в приложении 6.

2. Выполнение итоговой работы

Примерный перечень вопросов к зачету по дисциплине представлены в приложении 8.
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 представленой в приложении 7.

Очно-заочная форма обучения, Девятый семестр, Зачет

Контролируемые ИДК: ОПК-3.1 ОПК-3.2

Вопросы/Задания:

1. Работа с тестовыми заданиями

Тестовые задания представлены в приложении 6.

2. Выполнение итоговой работы

Примерный перечень вопросов к зачету по дисциплине представлены в приложении 8.
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 представленой в приложении 7.

Заочная форма обучения, Девятый семестр, Зачет

Контролируемые ИДК: ОПК-3.1 ОПК-3.2

Вопросы/Задания:

1. Работа с тестовыми заданиями

Тестовые задания представлены в приложении 6.

2. Выполнение итоговой работы

Примерный перечень вопросов к зачету по дисциплине представлены в приложении 8.
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 представленой в приложении 7.

10. Материально-техническое и учебно-методическое обеспечение дисциплины

10.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. Технологии обеспечения безопасности информационных систем: учебное пособие: учебное пособие / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов, М. О. Таныгин, Е. А. Кулешова. - Москва, Берлин: Директ-Медиа, 2021. - 210 с. - 978-5-4499-1671-6. - Текст: электронный. // Директ-Медиа: [сайт]. - URL: https://doi.org/10.23681/598988 (дата обращения: 26.09.2024). - Режим доступа: по подписке

Дополнительная литература

1. Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика: учебное пособие: учебное пособие / В. Я. Ищейнов. - Москва, Берлин: Директ-Медиа, 2020. - 271 с. - 978-5-4499-0496-6. - Текст: электронный. // Директ-Медиа: [сайт]. - URL: https://doi.org/10.23681/571485 (дата обращения: 26.09.2024). - Режим доступа: по подписке

2. Программно-аппаратные средства защиты информационных систем: учебное пособие: учебное пособие / Ю. Ю. Громов, О. Г. Иванова, К. В. Стародубов, А. А. Кадыков. - Тамбов: Тамбовский государственный технический университет (ТГТУ), 2017. - 194 с. - 978-5-8265-1737-6. - Текст: электронный. // Директ-Медиа: [сайт]. - URL: https://biblioclub.ru/index.php?page=book&id=499013 (дата обращения: 26.09.2024). - Режим доступа: по подписке

3. Закарюкин, В. П. Электромагнитная совместимость и средства защиты: учебное пособие: учебное пособие / В. П. Закарюкин, М. Л. Дмитриева, А. В. Крюков. - Москва, Берлин: Директ-Медиа, 2020. - 248 с. - 978-5-4499-1579-5. - Текст: электронный. // Директ-Медиа: [сайт]. - URL: https://doi.org/10.23681/598053 (дата обращения: 26.09.2024). - Режим доступа: по подписке

4. Басыня, Е. А. Системное администрирование и информационная безопасность: учебное пособие: учебное пособие / Е. А. Басыня. - Новосибирск: Новосибирский государственный технический университет, 2018. - 79 с. - 978-5-7782-3484-0. - Текст: электронный. // Директ-Медиа: [сайт]. - URL: https://biblioclub.ru/index.php?page=book&id=575325 (дата обращения: 26.09.2024). - Режим доступа: по подписке

5. Моргунов, А. В. Информационная безопасность: учебно-методическое пособие: учебно-методическое пособие / А. В. Моргунов. - Новосибирск: Новосибирский государственный технический университет, 2019. - 83 с. - 978-5-7782-3918-0. - Текст: электронный. // Директ-Медиа: [сайт]. - URL: https://biblioclub.ru/index.php?page=book&id=576726 (дата обращения: 26.09.2024). - Режим доступа: по подписке

6. Основы администрирования информационных систем: учебное пособие: учебное пособие / Д. О. Бобынцев, А. Л. Марухленко, Л. О. Марухленко, С. А. Кужелева, Л. А. Лисицын. - Москва, Берлин: Директ-Медиа, 2021. - 202 с. - 978-5-4499-1674-7. - Текст: электронный. // Директ-Медиа: [сайт]. - URL: https://doi.org/10.23681/598955 (дата обращения: 26.09.2024). - Режим доступа: по подписке

7. Основы информационной безопасности: учебник: учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев. - Москва: Юнити-Дана|Закон и право, 2018. - 287 с. - 978-5-238-02857-6. - Текст: электронный. // Директ-Медиа: [сайт]. - URL: https://biblioclub.ru/index.php?page=book&id=562348 (дата обращения: 26.09.2024). - Режим доступа: по подписке

10.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся

Профессиональные базы данных

1. http://www.ebiblioteka.ru - Базы данных East View
2. https://scholar.google.ru - Международная научная реферативная база данных

Ресурсы «Интернет»

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.edu.ru - Федеральный портал «Российское образование»
6. http://www.encyclopedia.ru - Мир энциклопедий
7. https://www.kaspersky.ru - Официальный сайт компании «Лаборатория Касперского»

10.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине

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» (http://www.biblioclub.ru).
2. Интегрированная библиотечно-информационная система ИРБИС64 (http://lib.sano.ru).
3. Справочно-правовая система КонсультантПлюс.
4. Электронная справочная система ГИС Омск.

10.4. Специальные помещения, лаборатории и лабораторное оборудование

Институт располагает материально-технической базой, соответствующей действующим противопожарным правилам и нормам и обеспечивающей проведение всех видов дисциплинарной и междисциплинарной подготовки, практической и научно-исследовательской работ обучающихся, предусмотренных учебным планом.
Для проведения учебных занятий по дисциплине используются следующие помещения, оснащенные оборудованием и техническими средствами обучения:

Для лекций, семинаров (практических), групповых, индивидуальных консультаций, текущего контроля, промежуточной аттестации, ГИА

Мультимедийная учебная аудитория № 210

Перечень оборудования
- Аудиоколонка - 5 шт.
- Доска маркерная - 1 шт.
- Компьютер с выходом в Интернет - 1 шт.
- Проектор - 1 шт.
- Стол - 37 шт.
- Стол преподавателя - 1 шт.
- Стул - 74 шт.
- Стул преподавателя - 1 шт.
- Трибуна - 1 шт.
- Экран - 1 шт.

Перечень программного обеспечения
(обновление производится по мере появления новых версий программы)
- Adobe Acrobat Reader
- Kaspersky Endpoint Security для Windows
- Microsoft Office 2007 standart Win32 Russian
- Microsoft Windows XP Professional Russian

Перечень информационно-справочных систем
(обновление выполняется еженедельно)
- Consultant Plus
- 2GIS

Мультимедийная учебная аудитория № 211

Перечень оборудования
- Аудиоколонка - 5 шт.
- Доска маркерная - 1 шт.
- Компьютер с выходом в Интернет - 1 шт.
- Проектор - 1 шт.
- Стол - 27 шт.

Стол преподавателя - 1 шт.
Стул - 54 шт.
Стул преподавателя - 1 шт.
Трибуна - 1 шт.
Экран - 1 шт.

Перечень программного обеспечения
(обновление производится по мере появления новых версий программы)
Adobe Acrobat Reader
Kaspersky Endpoint Security для Windows
Microsoft Office 2007 standart Win32 Russian
Microsoft Windows XP Professional Russian

Перечень информационно-справочных систем
(обновление выполняется еженедельно)
Consultant Plus
2GIS

Мультимедийная учебная аудитория № 304

Перечень оборудования
Аудиоколонка - 2 шт.
Доска маркерная - 1 шт.
Компьютер с выходом в Интернет - 1 шт.
Проектор - 0 шт.
Стол - 18 шт.
Стол преподавателя - 1 шт.
Стул - 36 шт.
Стул преподавателя - 1 шт.
Тематические иллюстрации - 0 шт.
Трибуна - 1 шт.
Учебно-наглядные пособия - 0 шт.
Экран - 0 шт.

Перечень программного обеспечения
(обновление производится по мере появления новых версий программы)
Adobe Acrobat Reader
Kaspersky Endpoint Security для Windows
Microsoft Office 2007 standart Win32 Russian
Microsoft Windows 10

Перечень информационно-справочных систем
(обновление выполняется еженедельно)
Consultant Plus
2GIS

Мультимедийная учебная аудитория № 312

Перечень оборудования
Аудиоколонка - 2 шт.
Компьютер с выходом в Интернет - 1 шт.
Проектор - 1 шт.
Тематические иллюстрации - 0 шт.
Учебно-наглядные пособия - 0 шт.
Экран - 1 шт.

Перечень программного обеспечения
(обновление производится по мере появления новых версий программы)
Adobe Acrobat Reader
Kaspersky Endpoint Security для Windows
Microsoft Office 2007 standart Win32 Russian
Microsoft Windows XP Professional Russian

Перечень информационно-справочных систем
(обновление выполняется еженедельно)
Consultant Plus
2GIS

Мультимедийная учебная аудитория № 422

Перечень оборудования
Аудиоколонка - 2 шт.
Доска маркерная - 1 шт.
Интерактивная доска - 1 шт.
Компьютер с выходом в Интернет - 1 шт.
Стол - 13 шт.
Стол преподавателя - 1 шт.
Стул - 26 шт.
Стул преподавателя - 1 шт.
Трибуна - 1 шт.

Перечень программного обеспечения
(обновление производится по мере появления новых версий программы)
Adobe Acrobat Reader
Kaspersky Endpoint Security для Windows
Microsoft Office 2007 standart Win32 Russian
Microsoft Windows 8 Professional Russian

Перечень информационно-справочных систем
(обновление выполняется еженедельно)
Consultant Plus
2GIS

Для семинаров (практических, лабораторных), консультаций, текущего контроля, промежуточной аттестации, ГИА, НИР, курсового проектирования

Лаборатория иностранных языков и информационных дисциплин № 401

Перечень оборудования
Доска маркерная - 1 шт.
Интерактивная доска - 1 шт.
Информационная доска - 1 шт.
Лингафонное оборудование - 0 шт.
Мультимедиапроектор - 1 шт.
Наушники с микрофоном - 10 шт.
Персональный компьютер - 11 шт.
Стол - 8 шт.
Стол преподавателя - 1 шт.
Стул - 16 шт.
Стул преподавателя - 1 шт.

Тематические иллюстрации - 0 шт.
Учебно-наглядные пособия - 0 шт.

Перечень программного обеспечения
(обновление производится по мере появления новых версий программы)
Adobe Acrobat Reader
Kaspersky Endpoint Security для Windows
Microsoft Office стандартный 2016
Microsoft Access 2016
Joy Class
NetBeansIDE
Microsoft Visual Studio 2017 CE (C#, C++)
Microsoft Visual Studio 2010 Express
Microsoft Visual Studio Community
Microsoft SQL 2010 Express
Notepad ++
MySQL
OracleSQLDeveloper
Microsoft SOAPToolkit
CADE
Denwer 3 webserver
Dev-C++
IDEEclipse
JDK 6
Freepascal
Lazarus
Geany
JavaDevelopmentKit
TheRProject
NetBeansIDE8
StarUML 5.0.2
EViews 9 StudentVersionLite
Gretl
Matrixer
Maxima
Xmind
BPWIN
IrfanView
SMARTBoard

Перечень информационно-справочных систем
(обновление выполняется еженедельно)
Consultant Plus
2GIS

Лаборатория экономических и информационных дисциплин № 402

Перечень оборудования
Доска маркерная - 1 шт.
Персональный компьютер - 10 шт.
Стол - 13 шт.
Стол преподавателя - 1 шт.
Стул - 16 шт.
Стул преподавателя - 1 шт.
Тематические иллюстрации - 0 шт.

Учебно-наглядные пособия - 0 шт.

Перечень программного обеспечения
(обновление производится по мере появления новых версий программы)
Adobe Acrobat Reader
Kaspersky Endpoint Security для Windows
NetBeansIDE
Microsoft Visual Studio 2017 CE (C#, C++)
Microsoft Visual Studio 2010 Express
Microsoft Visual Studio Community
Microsoft SQL 2010 Express
Notepad ++
MySQL
OracleSQLDeveloper
Microsoft SOAPToolkit
CADE
Denwer 3 webserver
Dev-C++
IDEEclipse
JDK 6
Freepascal
Lazarus
Geany
JavaDevelopmentKit
TheRProject
NetBeansIDE8
StarUML 5.0.2
EViews 9 StudentVersionLite
Gretl
Matrixer
Maxima
Xmind
BPWIN
IrfanView
SMARTBoard
Gimp
Java 8 Update 381 (64-bit)
Microsoft Office 2013 Professional Plus Win32 Russian
1С Предприятие 8.2. Комплект для обучения в высших и средних учебных заведениях
1С 8.2 АБС "Управление кредитной организацией"
Microsoft Project 2010

Перечень информационно-справочных систем
(обновление выполняется еженедельно)
Consultant Plus
2GIS

Лаборатория иностранных языков и информационных дисциплин № 403

Перечень оборудования
Доска маркерная - 1 шт.
Лингафонное оборудование - 0 шт.
Наушники с микрофоном - 10 шт.
Персональный компьютер - 11 шт.
Стол - 9 шт.

Стол преподавателя - 1 шт.
Стул - 21 шт.
Стул преподавателя - 1 шт.
Тематические иллюстрации - 0 шт.
Техническое оснащение (монитор) - 2 шт.
Учебно-наглядные пособия - 0 шт.

Перечень программного обеспечения
(обновление производится по мере появления новых версий программы)
Adobe Acrobat Reader
Kaspersky Endpoint Security для Windows
Microsoft Office 2007 standart Win32 Russian
NetBeansIDE
Microsoft Visual Studio 2017 CE (C#, C++)
Microsoft Visual Studio 2010 Express
Microsoft Visual Studio Community
Microsoft SQL 2010 Express
Notepad ++
MySQL
OracleSQLDeveloper
Microsoft SOAPToolkit
CADE
Denwer 3 webserver
Dev-C++
IDEEclipse
JDK 6
Freepascal
Geany
JavaDevelopmentKit
TheRProject
NetBeansIDE8
StarUML 5.0.2
EViews 9 StudentVersionLite
Gretl
Matrixer
Maxima
Xmind
BPWIN
IrfanView
NetClass
Microsoft Windows XP Professional Russian
CorelDRAW Graphics Suite X4
NetClass PRO
Gimp

Перечень информационно-справочных систем
(обновление выполняется еженедельно)
Consultant Plus
2GIS

Для лекций, семинаров (практических), групповых и индивидуальных консультаций, текущего контроля, промежуточной аттестации

Мультимедийная учебная аудитория № 305

Перечень оборудования
Аудиоколонка - 2 шт.
Доска маркерная - 1 шт.
Информационная доска - 1 шт.
Компьютер с выходом в Интернет - 1 шт.
Круглый стол - 3 шт.
Ноутбук DELL - 8 шт.
Ноутбук HP - 2 шт.
Персональный компьютер - 1 шт.
Проектор - 1 шт.
Стеллаж - 2 шт.
Стол одноместный - 10 шт.
Стол преподавателя - 1 шт.
Стул - 27 шт.
Стул преподавателя - 1 шт.
Трибуна - 1 шт.
Экран - 1 шт.

Перечень программного обеспечения
(обновление производится по мере появления новых версий программы)
MariaDB 10.11 (x64)
Microsoft Office 2016 standart Win64 Russian
Adobe Acrobat Reader
Kaspersky Endpoint Security для Windows

Перечень информационно-справочных систем
(обновление выполняется еженедельно)
Consultant Plus
2GIS

Помещение для хранения и профилактического обслуживания учебного, компьютерного оборудования и хранения элементов мультимедийных лабораторий

Специальное помещение № 420

Перечень оборудования
Запасные части для компьютерного оборудования - 0 шт.
Наушники для лингафонного кабинета - 0 шт.
Паяльная станция - 1 шт.
Персональный компьютер - 4 шт.
Планшетный компьютер - 15 шт.
Сервер - 10 шт.
Стеллаж - 0 шт.
Стол - 4 шт.
Стул - 4 шт.

Перечень программного обеспечения
(обновление производится по мере появления новых версий программы)
Не используется.

Перечень информационно-справочных систем
(обновление выполняется еженедельно)
Не используется.

Помещение для хранения и профилактического обслуживания учебного оборудования

Специальное помещение № 003

Перечень оборудования
Запасные части для столов и стульев - 0 шт.
Материалы для сопровождения учебного процесса - 0 шт.
Наборы слесарных инструментов для обслуживания учебного оборудования - 0 шт.
Станок для сверления - 0 шт.
Стеллаж - 0 шт.
Угловая шлифовальная машина - 0 шт.

Перечень программного обеспечения
(обновление производится по мере появления новых версий программы)
Не используется.

Перечень информационно-справочных систем
(обновление выполняется еженедельно)
Не используется.

Для семинаров (практических, лабораторных), консультаций, текущего контроля, промежуточной аттестации, курсового проектирования

Лаборатория иностранных языков и информационных дисциплин № 412

Перечень оборудования
Компьютер с выходом в Интернет - 11 шт.
Стол - 10 шт.
Стол преподавателя - 1 шт.
Стул - 10 шт.
Стул преподавателя - 1 шт.

Перечень программного обеспечения
(обновление производится по мере появления новых версий программы)
Adobe Acrobat Reader
Kaspersky Endpoint Security для Windows
Microsoft Visual Studio 2017 CE (C#, C++)
1С Предприятие 8.2. Комплект для обучения в высших и средних учебных заведениях
Microsoft Windows 10 Professional Russian
Microsoft Office профессиональный плюс 2016
7-Zip 24.08(x64)
Far Manager 3 (x64)
Microsoft Visual Studio Code
Python Launcher
PuTTY release 0.81 (64-bit)
PostgreSQL 16
PhpStorm 2024.2.0.1
PDF24 Creator 11.18.0
PyCharm Community Edition 2022.3.1
PyCharm Community Edition 2023.2.1
PyCharm Community Edition 2023.2.3
draw.io 24.7.5

Перечень информационно-справочных систем
(обновление выполняется еженедельно)
Не используется.

11. Методические указания по освоению дисциплины (модуля)

ВИДЫ И ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Успешное освоение теоретического материала по дисциплине требует самостоятельной работы, нацеленной на усвоение лекционного теоретического материала, расширение и конкретизацию знаний по разнообразным вопросам дисциплины. 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 отдельных 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. 5.1 или 5.2 рабочей программы дисциплины и обеспечить последовательное освоение теоретического материала по отдельным вопросам и темам (Приложение 2).

Наиболее целесообразен следующий порядок изучения теоретических вопросов по дисциплине:

1. Изучение справочников (словарей, энциклопедий) с целью уяснения значения основных терминов, понятий, определений;
2. Изучение учебно-методических материалов для лекционных, практических 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, представленными в электронной библиотеке института, и предназначенными для подготовки к лекционным и семинарским занятиям.

Контроль аудиторной самостоятельной работы осуществляется в форме дискуссии и собеседования. Контроль внеаудиторной самостоятельной работы студентов осуществляется в форме устного или письменного опроса. Промежуточный контроль знаний в форме экзамена

осуществляется посредством письменного тестирования, включающего вопросы и задания для самостоятельного изучения.

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).
Показатели и критерии оценивания компетенций на этапе текущего и промежуточного контроля представлены в Приложении 3.

Промежуточная аттестация по дисциплине проводится в форме экзамена/зачета 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 могут формироваться варианты тестов, относящихся ко всем темам дисциплины (Приложение 6)
Оценка знаний студентов осуществляется в соответствии с Положением о балльной и рейтинговой системах оценивания, принятой в Институте, и технологической картой дисциплины

ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ НА ЭТАПЕ ТЕКУЩЕГО КОНТРОЛЯ
1) 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.

2) 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 представленой в приложении 4.

3) 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 приложении 5.
Ход выполнения работы
1. Выберите вариант практического задания (приложение 5).
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.).

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 основана на использовании Положения о балльной и рейтинговой системах оценивания, принятой в институте, и технологической карты дисциплины.

Текущий контроль:
- посещение и работа на лекционных и практических занятиях (собеседование, контрольная работа, круглый стол и дискуссия) - 0-35 баллов;
- письменное задание (реферат) - 0-25 баллов;
- практическое задание (кейс) - 0-50 баллов.
Промежуточная аттестация:
- итоговая работа - 25 баллов.
Максимальное количество баллов по дисциплине – 100.
Максимальное количество баллов по результатам текущего контроля – 75.
Максимальное количество баллов на экзамене – 25.

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.

Описание возможностей изучения дисциплины лицами с ОВЗ и инвалидами

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		
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

Тематическое планирование самостоятельной работы студентов

Тема, раздел	Очная форма	Заочная форма	Очно-заочная форма	Задания для самостоятельной работы	Форма контроля
1. Основы информационной безопасности	6	22	16	- 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	16	- 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	16	- 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	16	- 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	64		

Приложение 3

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. 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.).	0-25

		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

Показатели и критерии оценивания компетенций на этапе промежуточной аттестации

№ 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

Приложение 4

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

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

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.

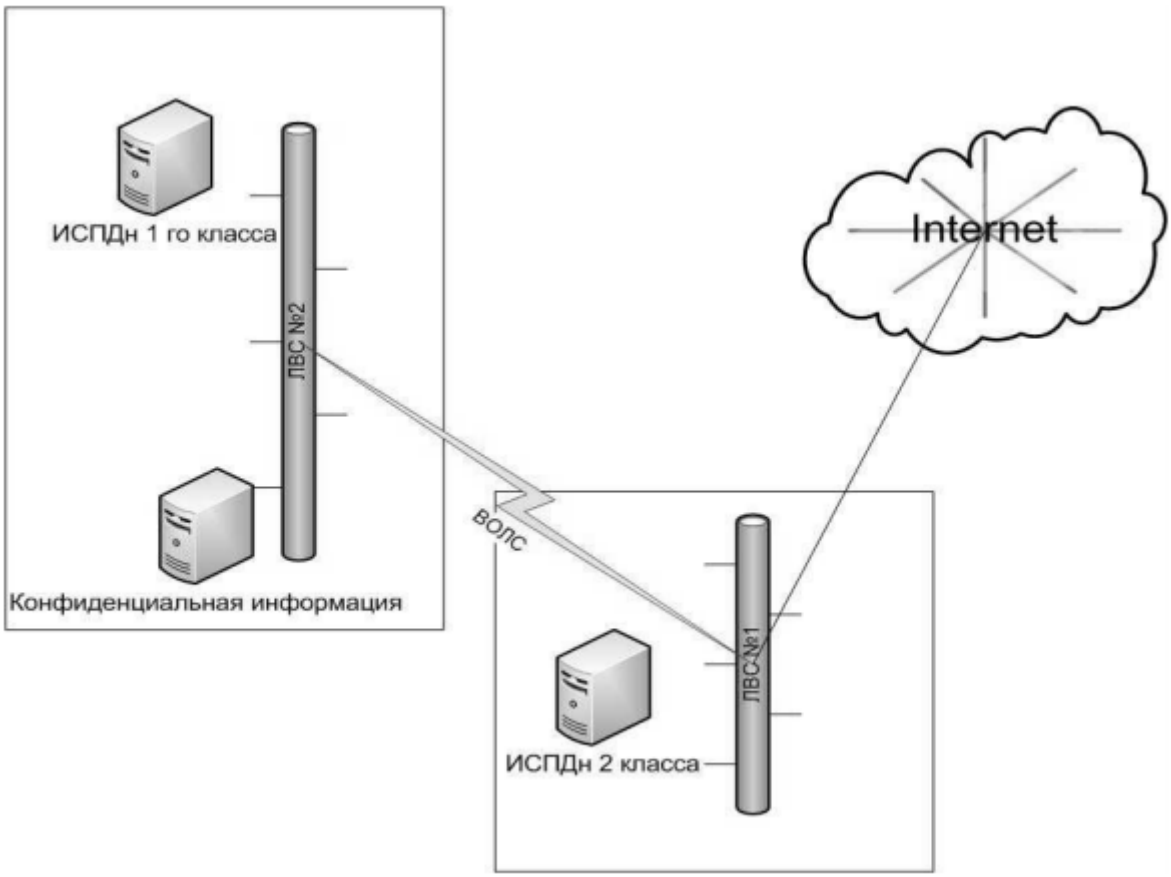

Рис. П1. Исходная схема для варианта 1

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.

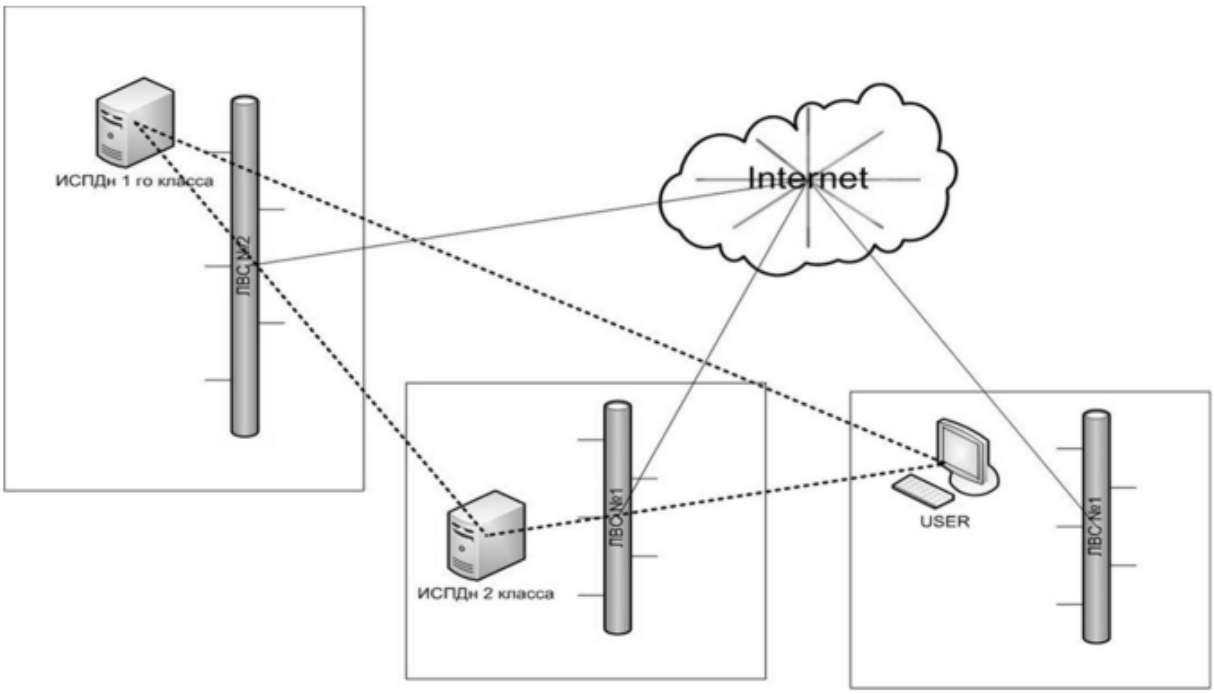

Рис. П2. Исходная схема для варианта 2

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.

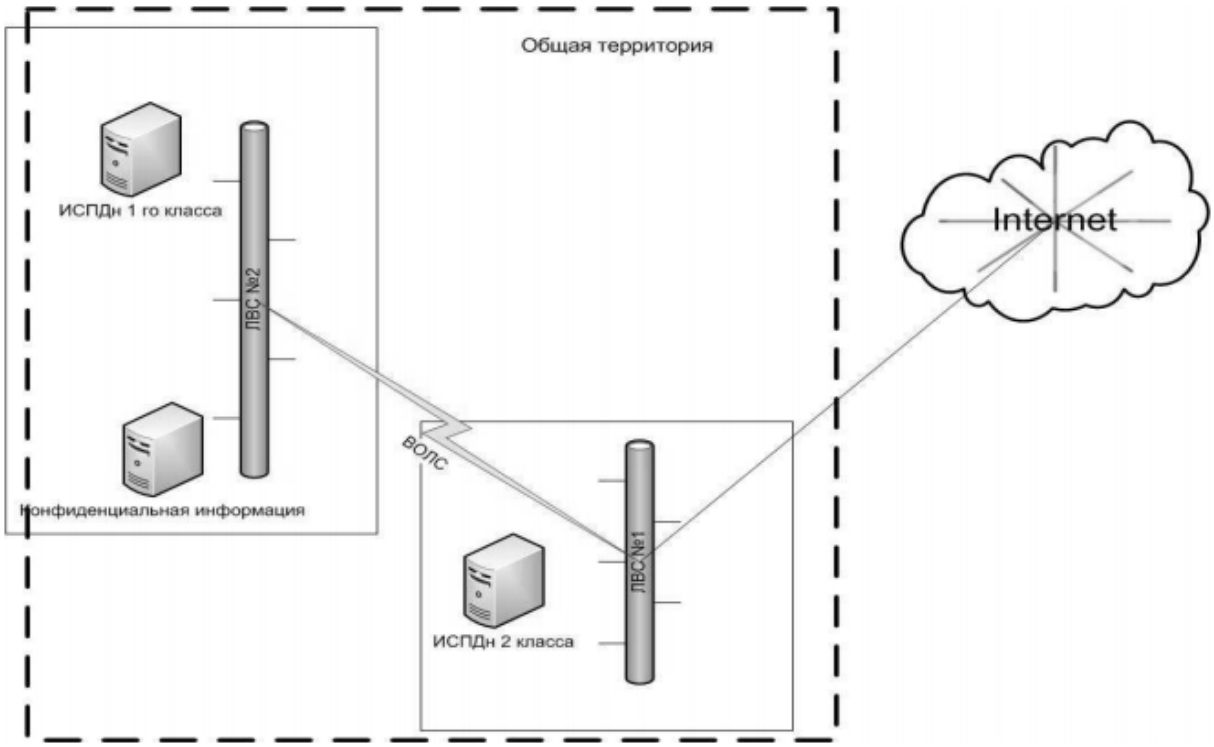

Рис. П3. Исходная схема к варианту 3

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.

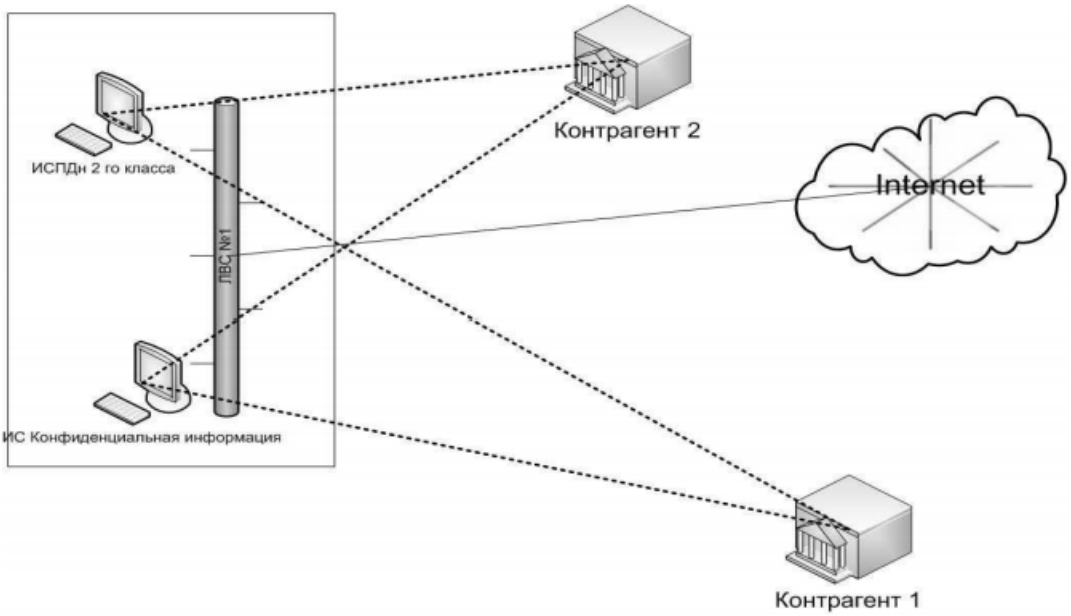

Рис. П4. Исходная схема к варианту

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.

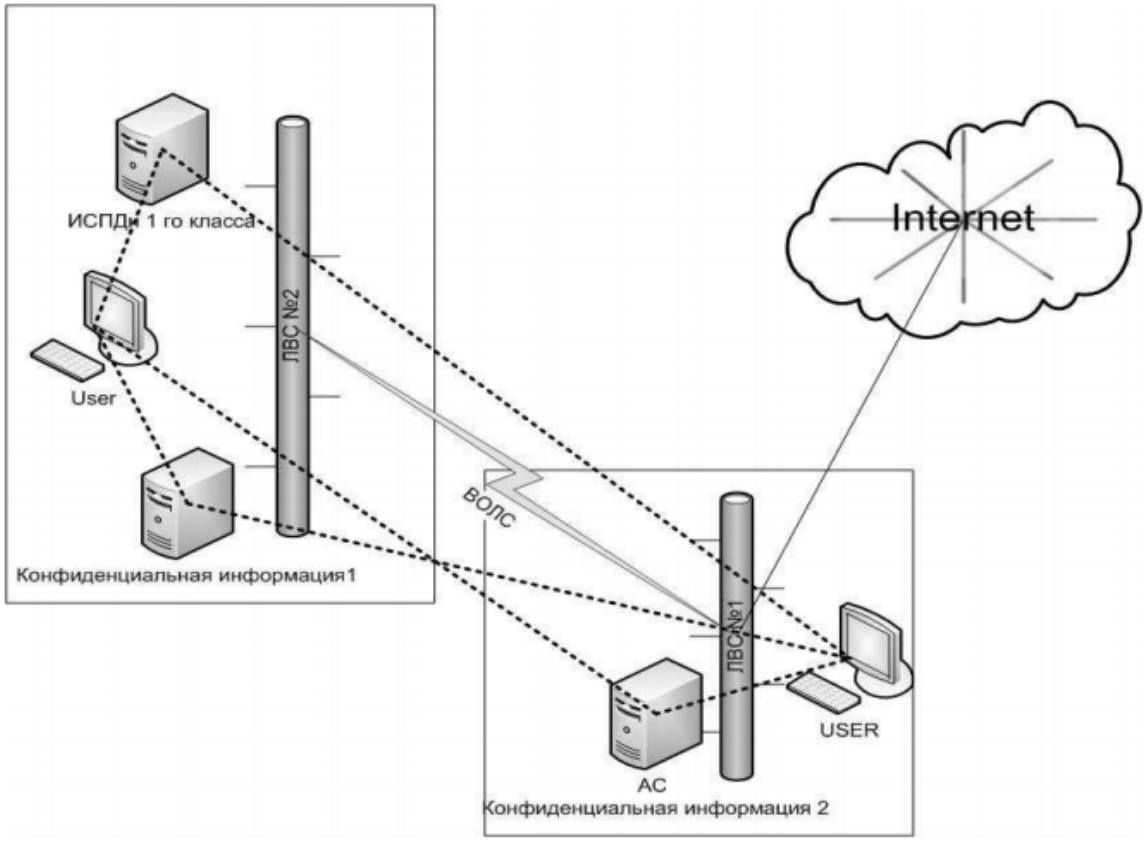

Рис. П5. Исходная схема к варианту 5

Приложение 6

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 7.

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

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.

Приложение 8

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.