МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета _____ / Баркалов С.А./

«17» января 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Информационная безопасность»

Направление подготовки 27.03.03 Системный анализ и управление

Профиль Бизнес-аналитика и системы больших данных

Квалификация выпускника бакалавр

Нормативный период обучения 4 года

Форма обучения очная

Год начала подготовки 2023

Автор программы _____ В.П. Морозов

Заведующий кафедрой Управления _____ С.А. Баркалов

Руководитель ОПОП _____ О.С. Перевалова

1.1. Цели дисциплины

изучение комплекса проблем информационной безопасности при подготовке данных и формировании требований к результатам аналитических работ в области анализа данных

1.2. Задачи освоения дисциплины

- знать способы защиты данных и перечень требований, предъявляемых к защите результатов аналитических работ в области анализа данных;
- уметь формулировать требования к защите результатов аналитических работ в области анализа данных;
- владеть навыками защиты данных и результатов аналитических работ в области анализа данных.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Информационная безопасность» относится к дисциплинам части, формируемой участниками образовательных отношений блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Информационная безопасность» направлен на формирование следующих компетенций:

УК-2 - Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

ПК-1 - Способен подготавливать данные и формировать требования к результатам аналитических работ в области анализа данных

Компетенция	Результаты обучения, характеризующие сформированность компетенции
УК-2	знать круг задач в области информационной безопасности в рамках предметной области бизнес-аналитики и систем больших данных
	уметь выбирать оптимальные способы решения задач в области информационной безопасности в рамках предметной области бизнес-аналитики и систем больших данных
	владеть навыками выбора и решения задач в области информационной безопасности в рамках предметной области бизнес-аналитики и систем больших данных
ПК-1	знать способы защиты данных и перечень требований, предъявляемых к защите результатов аналитических

	работ в области анализа данных
	уметь формулировать требования к защите результатов аналитических работ в области анализа данных
	владеть навыками защиты данных и результатов аналитических работ в области анализа данных

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Информационная безопасность» составляет 5 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры
		8
Аудиторные занятия (всего)	42	42
В том числе:		
Лекции	14	14
Практические занятия (ПЗ)	14	14
Лабораторные работы (ЛР)	14	14
Самостоятельная работа	111	111
Курсовая работа	+	+
Часы на контроль	27	27
Виды промежуточной аттестации - экзамен	+	+
Общая трудоемкость: академические часы зач.ед.	 180 5	 180 5

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Прак зан.	Лаб. зан.	СРС	Всего, час
1	Информационная безопасность в системе национальной безопасности Российской Федерации	Основные термины и определения. Классификация защищаемой информации. Некоторые проблемы обеспечения информационной безопасности в Российской Федерации. Основные положения документов «О стратегии национальной безопасности Российской федерации до 2030 года» и «Доктрина информационной безопасности Российской Федерации». Основные составляющие	4	2	4	18	28

		национальных интересов Российской Федерации в информационной сфере. Основные направления федерального законодательства в области защиты информации ограниченного доступа. Проблемы региональной информационной безопасности.					
2	Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем	Стандарты по оценке защищенных систем. Критерии безопасности компьютерных систем. Европейские «Критерии безопасности информационных технологий». Федеральные критерии безопасности информационных технологий. Канадские критерии безопасности компьютерных систем. Обзор серии стандартов ISO/IEC 17799. Стандарты ISO/IEC 17799:2002 (BS 7799:2000). Стандарт ISO/IEC 27001. Российский стандарт ГОСТ Р ИСО/МЭК 27001-2006. Стандарты ISO/IEC 15408 и ГОСТ Р ИСО/МЭК 15408. Российская классификация средств вычислительной техники и автоматизированных систем и требования по защите информации согласно РД ФСТЭК	2	2	2	18	24
3	Абстрактные модели обеспечения информационной безопасности	Ранние модели управления доступом. Модель матрицы доступов Харрисона – Руззо – Ульмана. Модель Белла и Лападула. Модель систем военных сообщений. Понятие контроля доступа, базирующегося на ролях	2	2	2	18	24
4	Основные угрозы информационной безопасности автоматизированных систем	Анализ и классификация угроз информационной безопасности автоматизированных систем. Причины, виды, каналы утечки и искажения информации. Угрозы программно-математических воздействий и нетрадиционных информационных каналов. Угрозы, основанные на информационных сетевых атаках	2	2	2	18	24
5	Основы построения систем защиты информации	Основные принципы обеспечения информационной безопасности предприятий. Основные методы и средства защиты информации. Порядок построения защищенной автоматизированных системах управления предприятия (АСУП). Аттестация объектов информатизации по требованиям безопасности информации	2	2	2	20	26
6	Основы обеспечения информационной безопасности в автоматизированных системах управления	Проблемы обеспечения информационной безопасности в АСУП. Основные термины и определения. Основные угрозы безопасности АСУП. Правовые основы защиты информации. Цели защиты информации. Режимы защиты информации. Классификация компьютерных преступлений	2	4	2	19	27
		Итого	**14**	**14**	**14**	**111**	**153**

5.2 Перечень лабораторных работ

1. Математические аспекты применения формальных моделей.
2. Практическая реализация и оценка формальных моделей.
3. Исследование корректности систем защиты.
4. Инсталляция и настройка штатных средств операционных систем, предназначенных для защиты от НСД и программно-аппаратных комплексов защиты от НСД.
5. Инсталляция и настройка МЭ, программно-аппаратных средств защиты информации при передаче по открытым каналам связи и разграничения доступа к сетевым ресурсам.
6. Анализ состояния информационных систем и организация защиты от хакерских атак.

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины предусматривает выполнение курсовой работы в 8 семестре для очной формы обучения.

Примерная тематика курсовой работы:

1. Комплексный подход к построению технической защиты информации на объекте информатизации.

2. Основные положения и принципы построения технической защиты информации.

3. Анализ демаскирующих признаков, методы и способы защиты демаскирующих признаков на объекте защиты.

4. Модель поведения внешнего нарушителя на этапах реализации угроз безопасности информации, методы и способы противодействия от утечки информации по техническим каналам.

5. Модель поведения инсайдера на этапах реализации угроз безопасности информации, методы и способы противодействия от утечки информации по техническим каналам.

6. Условия и факторы, способствующие утечки информации по техническим каналам, методы и способы противодействия утечке информации.

7. Условия и субъективные факторы, способствующие утечки информации по техническим каналам, методы и способы противодействия утечке информации.

8. Методы защиты видовых демаскирующих признаков от технических средств разведок.

9. Методы защиты сигнальных демаскирующих признаков от технических средств разведок.

10. Методы защиты радиосигналов от перехвата техническими средствами разведок.

11. Методы защиты электрических сигналов от перехвата техническими

средствами разведок.

12. Методы защиты материальных и вещественных демаскирующих признаков от технических средств разведок.

13. Технические средства наблюдения в видимом и ИК диапазонах за объектом защиты, методы и средства противодействия средствам наблюдения.

14. Технические средства наблюдения в радио диапазонах за объектом защиты, методы и средства противодействия средствам наблюдения.

15. Технические средства перехвата конфиденциальной информации передаваемой по линии связи, методы и средства противодействия перехвата конфиденциальной информации.

Задачи, решаемые при выполнении курсовой работы:

• закрепить знания, полученные на лекциях;

• научиться корректно работать с научной литературой;

• сформировать багаж знаний для выполнения выпускной квалификационной работы.

Курсовая работа включат в себя графическую часть и расчетно-пояснительную записку.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

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

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован»;

«не аттестован».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
УК-2	знать круг задач в области информационной безопасности в рамках предметной области бизнес-аналитики и систем больших данных	Сформированные представления о круге задач в области информационной безопасности в рамках предметной области бизнес-аналитики и систем больших данных	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь выбирать оптимальные способы решения задач в области информационной безопасности в рамках предметной	Способен подобрать рациональные методики и способы решения задач в области информационной безопасности в рамках предметной области бизнес-аналитики и систем больших данных	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	области бизнес-аналитики и систем больших данных			
	владеть навыками выбора и решения задач в области информационной безопасности в рамках предметной области бизнес-аналитики и систем больших данных	Демонстрирует навыки решения задач в области информационной безопасности в рамках предметной области бизнес-аналитики и систем больших данных	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-1	знать способы защиты данных и перечень требований, предъявляемых к защите результатов аналитических работ в области анализа данных	Сформированные представления о способах защиты данных и перечне требований, предъявляемых к защите результатов аналитических работ в области анализа данных	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь формулировать требования к защите результатов аналитических работ в области анализа данных	Демонстрирует навыки формулировки требований к защите результатов аналитических работ в области анализа данных	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыками защиты данных и результатов аналитических работ в области анализа данных	Демонстрирует навыки реализации последовательности защиты данных и результатов аналитических работ в области анализа данных	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 8 семестре для очной формы обучения по четырехбалльной системе:

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл.	Неудовл.
УК-2	знать круг задач в области информационной	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных

	безопасности в рамках предметной области бизнес-аналитики и систем больших данных					ответов
	уметь выбирать оптимальные способы решения задач в области информационной безопасности в рамках предметной области бизнес-аналитики и систем больших данных	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	владеть навыками выбора и решения задач в области информационной безопасности в рамках предметной области бизнес-аналитики и систем больших данных	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
ПК-1	знать способы защиты данных и перечень требований, предъявляемых к защите результатов аналитических работ в области анализа данных	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь формулировать требования к защите результатов аналитических работ в области анализа данных	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	владеть навыками защиты данных и результатов аналитических работ в области анализа данных	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 Примерный перечень заданий для подготовки к тестированию

1. Укажите основные свойства VPN

Создает туннель, т.е. защищённый канал передачи данных
Использует шифрование данных
Реализуется в незащищенных или слабо защищенных сетях

2. Каковы функциональные возможности программы Retina WiFi Scanner

Вычисляет WEP-ключи методом brute force
Генерирует отчёты
Обнаруживает IP-адреса и другую сетевую информацию
Обнаруживает неавторизованные беспроводные устройства

3. 64- и 128-битное WEP-шифрование трафика на основе RC4 обеспечивает уровень безопасности

Высокий

4. Отметьте потенциально опасные с точки зрения утечек внутренней информации действия

Размещение серверов в стороннем дата-центре
Хранение носителей вне офиса
Сервисный ремонт серверов или жестких дисков
Перевозка компьютеров или носителей

5. Перебор всех слов языка для взлома пароля это

атака Brute Force

7. Какого типа БД является реестр

иерархическая

8. IDS - это

система обнаружения вторжений

9. Какие режимы работы имеет программа Iris

Decode
Capture

10. Используется ли VPN для защиты беспроводных сетей

да

11. Какие дополнительные меры обеспечения безопасности могут использоваться в беспроводных сетях

Технология VPN
Использование IPSec для защиты трафика
Защита беспроводного сегмента с помощью L2TP

Выделение беспроводной сети в отдельный сегмент

12.Инсайдер - это

член какой-либо группы людей, имеющий доступ к секретной, скрытой или какой-либо другой закрытой информации или знаниями, недоступной широкой публике

13.Сколько root key содержит реестр Windows

5

14.Решение DeviceLock является

программно-аппаратным

15.Способ построения одноранговых Wi-Fi сетей называется

Ad-hoc

16.Какие решения применяются для контроля доступа к внешним устройствам

Secret Disk
ZLock
DeviceLock

7.2.2 Примерный перечень заданий для решения стандартных задач

1. Компьютер проверяет 10 млн. паролей в секудну. Сколько примерно времени ему потребуется, чтобы проверить методом словарной атаки все пароли для языка, содержащего 1 млн слов

0,1 секунды

2. Сколько групп символов должен минимально содержать надежный пароль

3

3. Тонкий клиент - это

Бездисковый компьютер-клиент в сетях с клиент-серверной или терминальной архитектурой, который переносит все или большую часть задач по обработке информации на сервер

4. В какой блок файла autorun.inf обычно прописываются вредоносные программы

open

5. Каково количество популярных паролей, которые остаются неизменными в течение последних 15 лет

500

6. Какой протокол VPN используется для создания защищенного сегмента локальной сети

IpSec

7. DLP (Data Leak Prevention) система защищает от

утечек конфиденциальной информации из информационной системы вовне

8. Что позволяет выполнять программа Process Monitor

Отслеживать сетевую активность процесса
Отслеживать обращение процесса к реестру
Отслеживать работу процесса с файлами

9. Необходимы ли криптографические ключи для создания VPN-тоннеля

Да

10. Каковы предпосылки возникновения систем защиты информации?

-появление ЭВМ
-развитие кибернетики, математики, философии, психологии и т.д.
-научная фантастика
-нет правильного ответа

7.2.3 Примерный перечень заданий для решения прикладных задач

1. Файл рабочей группы MS Access содержит следующие встроенные учётные записи:

-System, Window, Help
-Search, View, Copy
-Run, Project, Tools
-Database, Win32, Standart
+Admins, Admin, Users

2. Для создания новой рабочей группы в MS Access запускаем программу

+wrkgadmexe
-wrkgadmmdw
-wrkgadmmdb
-wrkgadmcpp
-wrkgadmdoc

3. Как называется документ в программе MS Access?

-таблица
+база данных
-книга
-форма

4. Телефонный радио ретранслятор большой мощности работает в

диапазоне?
+65-108 МГц
-65-80 Мгц
-27-28 МГц
-88-108МГц
-30 МГц

5. Речевой сигнал находится в диапазоне…
+200300 Гц до 46 кГц
-200…400 Гц до 2…6 кГц
-100…300 Гц до 4…6 кГц
-200…300 Гц до 2…6 кГц
-200…400 Гц до 4…6 кГц

6. Телефонный ретранслятор с питанием от телефонной линии имеет выходную мощность
-10 мВт
-5 мВт
+20 мВт
-30 мВт
-15 мВт

7. Телефонный радио ретранслятор с ЧМ на одном транзисторе обеспечивает дальность передачи
-До 100 м
+До 200м
-До 300м
-До 50м
-До 400м

8. Телефонный ретранслятор УКВ диапазона с ЧМ его дальность действия передатчика
+Около 100м
-Около 200м
-Около 300м
-Около 400м
-Около 50м

9. Отличие конвертера от Миниатюрного конвертера на частоте 430 МГц.
+Позволяет принимать сигнал с частотой до 1 ГГц
-Емкостью С1 до 15 пФ
-Способу подсоединения к телефонной линии
-Позволяет прослушивать телефонный разговор в диапазона 27-28 МГц
Источник: https://yznaika.com/notes/501

10 Чтобы установить парольную защиту в ОС Windows , необходимо выполнить следующую процедуру?
+Пуск->Панель управления->Учетные записи->Изменение пароля
-Пуск->Учетные записи->Изменение пароля
-Пуск->Справка->Учетные записи->Изменение пароля

-Пуск->Панель управления->Пароли и данные->Изменение пароля

7.2.4 Примерный перечень вопросов для подготовки к зачету

Не предусмотрено учебным планом

7.2.5 Примерный перечень заданий для подготовки к экзамену

1. Каким образом десять неформальных свойств модели СВС реализуются в ее формальном описании?

2. В каком случае система (T, s0) безопасна?

3. Где в определениях безопасности модели СВС реализовано ss-свойство безопасности классической модели Белла-ЛаПадулы?

4. Где в определениях безопасности модели СВС реализовано *-свойство безопасности классической модели Белла-ЛаПадулы?

5. Где в определениях безопасности модели СВС реализовано ds-свойство безопасности классической модели Белла-ЛаПадулы?

6. Каким стандартам необходимо следовать при построении СУИБ?

7. Что регламентируется в стандарте ISO 27002?

8. Что регламентируется в стандарте ISO 18044?

9. Что должна обеспечивать СУИБ?

10. Какова главная задача СУИБ?

11. Какой вид политики управления доступом используется в качестве основы автоматной модели безопасности информационных потоков?

12. В каких случаях в КС с мандатным управлением доступом нецелесообразно предотвращение возможности реализации всех информационных потоков от устройств ввода пользователей с высоким уровнем доступа к устройствам вывода пользователей с низким уровнем доступа?

13. В чем отличие информационной невыводимости от информационного невлияния?

14. Почему использование определения требований информационного невлияния (с учетом времени) позволяет обеспечить возможность функционирования в КС монитора ссылок?

15. В каких случаях может являться эффективным моделирование безопасности информационных потов с использованием вероятностных подходов?

16. Что понимается под термином информационная безопасность?

17. Что понимается под термином доступность информации?

18. Что понимается под термином целостность информации?

19. Что понимается под термином конфиденциальность информации?

20. Что понимается под термином комплекс средств автоматизации обработки информации?

21. Что понимается под термином информационная безопасность ИС?

22. Что понимается под термином уничтожение информации?

23. Какие способы защиты от вирусов Вы знаете?

24. Какие способы защиты от несанкционированного доступа Вы можете привести?

25. Анализ источников, каналов распространения и каналов утечки

информации (на примере конкретной фирмы).

26. Анализ конкретной автоматизированной системы, предназначенной для обработки и хранения информации о конфиденциальных документах

фирмы.

27. Основы технологии обработки и хранения конфиденциальных документов (по зарубежной литературе).

28. Назначение, виды, структура и технология функционирования системы защиты информации.

29. Поведение персонала и охрана фирмы в экстремальных ситуациях различных типов.

30. Аналитическая работа по выявлению каналов утечки информации фирмы.

31. Анализ функций секретаря-референта небольшой фирмы в области защиты информации.

32. Направления и методы защиты профессиональной тайны.

33. Направления и методы защиты служебной тайны.

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

Оценка «отлично» выставляется студентам, успешно сдавшим экзамен, и показавшим глубокое знание теоретической части курса, умение проиллюстрировать изложение практическими приемами и расчетами, проявившим творческие способности в понимании, изложении и использовании учебно-программного материала, полно, подробно ответившим на вопросы билета и экзаменатора;

Оценка «хорошо» выставляется студентам, сдавшим экзамен с незначительными замечаниями, и показавшим глубокое знание теоретической части курса, умение проиллюстрировать изложение практическими приемами и расчетами, освоившим основную литературу, рекомендованную программой курса, обнаружившим стабильный характер знаний и способность к их самостоятельному восполнению и обновлению в ходе практической деятельности, полностью ответившим на вопросы билета и вопросы экзаменатора, но допустившим при ответах незначительные ошибки, указывающие на наличие несистематичности и пробелов в знаниях;

Оценка «удовлетворительно» выставляется студентам, сдавшим экзамен со значительными замечаниями, показавшим знание основных положений теории при наличии существенных пробелов в деталях, испытывающим затруднения при практическом применении теории, допустившим существенные ошибки при ответах на вопросы билетов и вопросы экзаменатора, но показавшим знания основного учебно-программного материала в объеме, необходимом для предстоящей работы;

Оценка «неудовлетворительно» выставляется, если студент показал существенные пробелы в знаниях основных положений теории, которые не позволяют ему приступить к практической работе без дополнительной

подготовки, не ответил на вопросы билеты или членов экзаменационной комиссии.

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Информационная безопасность в системе национальной безопасности Российской Федерации	УК-2, ПК-1	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
2	Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем	УК-2, ПК-1	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
3	Абстрактные модели обеспечения информационной безопасности	УК-2, ПК-1	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
4	Основные угрозы информационной безопасности автоматизированных систем	УК-2, ПК-1	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
5	Основы построения систем защиты информации	УК-2, ПК-1	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
6	Основы обеспечения информационной безопасности в автоматизированных системах управления	УК-2, ПК-1	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи

компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Защита курсовой работы, курсового проекта или отчета по всем видам практик осуществляется согласно требованиям, предъявляемым к работе, описанным в методических материалах. Примерное время защиты на одного студента составляет 20 мин.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

1. Баркалов С.А., Белоусов В.Е., Колодяжный С.А. Информационная безопасность при управлении техническими системами:/ Учебное пособие. Санкт-Петербург: Изд-во Интермедия, 2016. – 528 с.

2. *Белоусов В.Е.* Средства защиты информации в интегрированных технических системах управления. Методические указания для выполнения курсового проекта [Электронный]// В.Е.Белоусов. Воронеж. гос. арх.–строит. ун–т. -Воронеж, 2014.- 42 с.

3. *Белоусов В.Е.* Средства защиты информации в интегрированных технических системах управления. Методические указания по самостоятельной работе [Электронный]// Е.Белоусов. Воронеж. гос. арх.–строит. ун–т. -Воронеж, 2014.- 33 с.

4. Громыко, И.А. Общая парадигма защиты информации. Определение терминов: от носителей к каналам утечки информации // Защита информации. Инсайд. – 2008. - № 1. – С.12-15.

5. Доля, А.А. Внутренние ИТ-угрозы в России – 2006 // Защита информации. Инсайд. – 2007. - № 2. – С.60-69.

6. Зенин, Н. Обеспечение конфиденциальности информации – это всегда комплексный подход // Трудовое право. – 2010. – № 1. – С. 41-42.

7. Камаев, В.А., Натров, В.В. Моделирование и анализ состояния информационной безопасности организации // Защита информации. Инсайд. – 2009. - № 4. – С.16-20.

8. Суханова, И.М. Аттестация и комплексная оценка персонала // Кадровые решения. – 2007. - № 4. – С.76-84.

9. Чуковенков, А.Ю. Документы по аттестации служащих // Секретарь-референт. – 2006. - № 11. – С. 17-23.

10. Шубин, А.С. Наша Тайна громко плачет… // Защита информации. Инсайд. – 2008. - № 1. С. 19-27.

11. Янковая, В.Ф. Гриф ограничения доступа к документу // Секретарь-референт. – 2008. - № 1. – С. 17-19.

12. Янковая, В.Ф. Организация конфиденциального делопроизводства // Секретарь-референт. – 2009. - № 12. – С.17 – 20.

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

1. Единое окно доступа к образовательным ресурсам. Электронная библиотека [Электронный ресурс]: инф. система. – М.: ФГАУ ГНИИ ИТТ "Информика", 2005-2012. – Режим доступа: //www. http://window.edu.ru, свободный. – Загл. с экрана (дата обращения 27.08.2021)
2. Интернет-университет информационных технологий – дистанционное образование – INTUIT.ru [Электронный ресурс]: офиц. сайт. – М.: Открытые системы, 2003-2011. - Режим доступа: http://www.intuit.ru, свободный. - Загл. С экрана (дата обращения: 27.08.2021).
3. Поисковые системы: Google, Yandex, Rambler.
4. Электронно-библиотечная система Издательство «Лань» [Электронный ресурс], СПб.: Издательство Лань, 2014. Режим доступа: http://e.lanbook.com. – Загл. с экрана (дата обращения 27.08.2021).

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

1. Компьютерные классы, которые позволяют реализовать образовательные возможности с доступом в сеть Интернет на скорости 6 мегабит в секунду. С возможностью проводить групповые занятия с обучаемыми, а также онлайн (оффлайн) тестирование.
2. Библиотечный электронный читальный зал с доступом к электронным ресурсам библиотек страны и мира. В количестве 3-х мест.
3. Персональные компьютеры с предустановленным лицензионным программным обеспечением не ниже Windows 7, Office 2007, которое позволяет работать с видео-аудио материалами, создавать и демонстрировать презентации, с выходом в сеть Интернет
4. Ноутбуки с предустановленным лицензионным программным обеспечением не ниже Windows 7, Office 2007, которое позволяет работать с видео-аудио материалами, создавать и демонстрировать презентации, с выходом в сеть Интернет.

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Информационная безопасность» читаются лекции, проводятся практические занятия и лабораторные работы, выполняется курсовая работа.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Практические занятия направлены на приобретение практических

навыков расчета. Занятия проводятся путем решения конкретных задач в аудитории.

Лабораторные работы выполняются на лабораторном оборудовании в соответствии с методиками, приведенными в указаниях к выполнению работ.

Методика выполнения курсовой работы изложена в учебно-методическом пособии. Выполнять этапы курсовой работы должны своевременно и в установленные сроки.

Контроль усвоения материала дисциплины производится проверкой курсовой работы, защитой курсовой работы.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Практическое занятие	Конспектирование рекомендуемых источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы. Прослушивание аудио- и видеозаписей по заданной теме, выполнение расчетно-графических заданий, решение задач по алгоритму.
Лабораторная работа	Лабораторные работы позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности лабораторных для подготовки к ним необходимо: следует разобрать лекцию по соответствующей теме, ознакомится с соответствующим разделом учебника, проработать дополнительную литературу и источники, решить задачи и выполнить другие письменные задания.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточной аттестации.
Подготовка к промежуточной аттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед экзаменом три дня эффективнее всего использовать для повторения и систематизации материала.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Перечень вносимых изменений	Дата внесения изменений	Подпись заведующего кафедрой, ответственной за реализацию ОПОП