МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета _____ Гусев П.Ю.

«31» августа 2021 г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«Основы информационной безопасности»

Специальность 10.05.03 Информационная безопасность автоматизированных систем

Специализация специализация N 7 "Анализ безопасности информационных систем"

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2021

Автор программы _____ /О.Н. Чопоров/

Заведующий кафедрой
Систем информационной
безопасности _____ /А.Г. Остапенко/

Руководитель ОПОП _____ / А.Г. Остапенко /

Воронеж 2021

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины: обеспечить будущими инженерам, базовые знания и умения в области информационной безопасности для изучения последующих дисциплин

1.2. Задачи освоения дисциплины

- знакомство с профессиональной терминологией в области информационной безопасности;
- системное знакомство с проблематикой обеспечения информационной безопасности;
- знакомство с местом и ролью информационной безопасности в системе национальной безопасности Российской Федерации, основами государственной информационной политики;
- знакомство с нормативно-правовой базой в области информационной безопасности;
- знакомство с классификацией угроз и уязвимостей информационной безопасности;
- знакомство с типовыми каналами утечки информации и средствами их обнаружения;
- знакомство с основными средствами и способами обеспечения информационной безопасности, принципами построения систем защиты информации;
- знакомство с методами компьютерно-технической экспертизы.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Основы информационной безопасности» относится к дисциплинам обязательной части блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Основы информационной безопасности» направлен на формирование следующих компетенций:

ОПК-1 - Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ОПК-1	Знать: - сущность и понятие информационной безопасности, характеристику ее составляющих - место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной

	политики; - основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.
	Уметь - классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; - классифицировать и оценивать угрозы информационной безопасности

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Основы информационной безопасности» составляет 3 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры
		2
Аудиторные занятия (всего)	36	36
В том числе:		
Лекции	18	18
Практические занятия (ПЗ)	18	18
Самостоятельная работа	72	72
Виды промежуточной аттестации - зачет	+	+
Общая трудоемкость: академические часы зач.ед.	 108 3	 108 3

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.	СРС	Всего, час
1	Основные понятия и задачи информационной безопасности.	Классификация информации по режиму доступа, защита информации. Система менеджмента информационной безопасности (СМИБ), активы, угрозы и уязвимости, инцидент информационной безопасности, ущерб, риск, менеджмент риска ИБ, защитные меры. Понятие информационной безопасности и его составляющие.	2	2	2	6
2	Информационная безопасность Российской Федерации	Угрозы информационной безопасности Российской Федерации. Доктрина информационной безопасности. Общая структура государственной системы обеспечения информационной безопасности Российской Федерации. Общие принципы защиты информации.	2	2	4	8
3	Международная, национальная и ведомственная нормативная	Виды нормативно-правового и справочного обеспечения в области информационной безопасности. Концептуальные документы в	2	2	14	18

	правовая база в области информационной безопасности	области информационной безопасности. Нормативно-правовые акты Российской Федерации (кодексы, Федеральные законы РФ, Постановления Правительства РФ, Указы президента РФ, Нормативные документы и инструктивные материалы ФСТЭК (Гостехкомиссии) России)				
4	Безопасность (защищенность) компьютерных систем	Классификация угроз. Методы нарушения секретности, целостности и доступности информации. Модели управления доступом. Обзор средств и методов информационной/компьютерной безопасности. Модель действий вероятного нарушителя и модель построения защиты. Классификация основных видов атак. Сетевая разведка. Средства и методы для нейтрализации атак.	2	2	12	16
5	Вредоносное программное обеспечение	Классификация вредоносных программ. Признаки присутствия вредоносного ПО. Методы защиты. Методы обнаружения. Способы внедрения. Примеры сетевых атак. Троянские программы, люки, эксплойты. Технологии самозащиты. Место и роль межсетевых экранов (МЭ) в обеспечении безопасности ресурсов АС. Возможности и ограничения антивирусных программ. Специализированные средства и методы выявления вредоносных программ.	2	2	8	12
6	Средства защиты и нападения	Информационная война и информационное оружие. Особенности технических средств информационной войны. Классификация средств защиты и нападения. Классификация электронных устройств перехвата информации, внедряемых в средства вычислительной техники. Средства силового деструктивного воздействия (СДВ).	2	2	8	12
7	Уничтожение информации	Необходимость уничтожения документов. Особенности удаления информации с электронных носителей. Политика уничтожения данных. Уничтожение конфиденциальной информации (плановое и экстренное). Следы в сети. Уникальные идентификаторы интернет-пользователей и электронные "отпечатки". Конфиденциальность в социальных сетях.	2	2	8	12
8	Защита информации от утечки по техническим каналам	Утечки: понятие, виды. Типовые каналы утечки информации. Технические каналы утечки. Средства и методы обнаружения технических каналов утечки информации. Системы защиты конфиденциальных данных от внутренних угроз. Технология цифровых отпечатков.	2	2	8	12
9	Компьютерно-техническая экспертиза	Компьютерно-техническая экспертиза. Методы экспертизы. Проведение расследования компьютерных инцидентов. Исследование носителей компьютерной информации. Аппаратно-программные средства расследования компьютерных инцидентов.	2	2	8	12
		Итого	**18**	**18**	**72**	**108**

5.2 Перечень лабораторных работ

Не предусмотрено учебным планом

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

В соответствии с учебным планом освоение дисциплины не предусматривает выполнение курсового проекта (работы) или контрольной работы.

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».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ОПК-1	Знать: - сущность и понятие информационной безопасности, характеристику ее составляющих - место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики; - основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.	знает сущность и понятие информационной безопасности, характеристику ее составляющих; знает место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики; знает основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь - классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; - классифицировать и оценивать угрозы информационной безопасности	умеет классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; умеет классифицировать и оценивать угрозы информационной безопасности	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 2 семестре для очной формы обучения по двухбалльной системе:

«зачтено»

«не зачтено»

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Зачтено	Не зачтено
ОПК-1	Знать: - сущность и понятие информационной безопасности, характеристику ее	Тест	Выполнение теста на 70-100%	Выполнение менее 70%

	составляющих - место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики; - основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.			
	Уметь - классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; - классифицировать и оценивать угрозы информационной безопасности	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены

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. Информация это -

- сведения, поступающие от СМИ
- только документированные сведения о лицах, предметах, фактах, событиях
- **сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления**
- только сведения, содержащиеся в электронных базах данных

2. Информация, зафиксированная на материальном носителе, с реквизитами,позволяющими ее идентифицировать, называется

- достоверной
- конфиденциальной
- **документированной**
- коммерческой тайной

3. Формы защиты интеллектуальной собственности -

- **авторское, патентное право и коммерческая тайна**
- интеллектуальное право и смежные права
- коммерческая и государственная тайна
- гражданское и административное право

4. По доступности информация классифицируется на

- открытую информацию и государственную тайну
- конфиденциальную информацию и информацию свободного доступа
- **информацию с ограниченным доступом и общедоступную**

информацию

- виды информации, указанные в остальных пунктах

5. К конфиденциальной информации относятся документы, содержащие

- государственную тайну

- законодательные акты
- "ноу-хау"
- сведения о золотом запасе страны

6. Запрещено относить к информации ограниченного доступа

- информацию о чрезвычайных ситуациях
- информацию о деятельности органов государственной власти
- документы открытых архивов и библиотек
- **все, перечисленное в остальных пунктах**

7. К конфиденциальной информации не относится

- коммерческая тайна
- персональные данные о гражданах
- государственная тайна
- **"ноу-хау"**

8. Вопросы информационного обмена регулируются (...) правом

- **гражданским**
- информационным
- конституционным
- уголовным

9. Конфиденциальная информация это

- сведения, составляющие государственную тайну
- сведения о состоянии здоровья высших должностных лиц
- **документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ**
- данные о состоянии преступности в стране

10. Какая информация подлежит защите?

- информация, циркулирующая в системах и сетях связи
- зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать
- только информация, составляющая государственные информационные ресурсы
- **любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу**

7.2.2 Примерный перечень заданий для решения стандартных задач

1. Система защиты государственных секретов определяется Законом

- "Об информации, информатизации и защите информации"
- "Об органах ФСБ"
- **"О государственной тайне"**
- "О безопасности"

2. Классификация и виды информационных ресурсов определены

- **Законом "Об информации, информатизации и защите информации"**
- Гражданским кодексом
- Конституцией
- всеми документами, перечисленными в остальных пунктах

3. Формой правовой защиты литературных, художественных и научных произведений является (...) право

- литературное
- художественное
- **авторское**
- патентное

4. Запрещено относить к информации с ограниченным доступом

- **законодательные акты, информацию о чрезвычайных ситуациях и информацию о деятельности органов государственной власти (кроме государственной тайны)**
- только информацию о чрезвычайных ситуациях
- только информацию о деятельности органов государственной власти (кроме государственной тайны)
- документы всех библиотек и архивов

5. К коммерческой тайне могут быть отнесены

- сведения не являющиеся государственными секретами
- сведения, связанные с производством и технологической информацией
- сведения, связанные с управлением и финансами
- **сведения, перечисленные в остальных пунктах**

6. Какой законодательный акт содержит сведения по защите коммерческой тайны?

- Закон "Об авторском праве и смежных правах"
- **Закон "О коммерческой тайне"**
- Патентный закон
- Закон "О правовой охране программ для ЭВМ и баз данных"

7. К информации ограниченного доступа не относится

- государственная тайна
- размер золотого запаса страны
- **персональные данные**
- коммерческая тайна

8. Система защиты государственных секретов

- основывается на Уголовном Кодексе РФ
- регулируется секретными нормативными документами
- **определена Законом РФ "О государственной тайне"**
- осуществляется в соответствии с п.1-3

9. Документы, содержащие государственную тайну снабжаются грифом

- "секретно"
- "совершенно секретно"

- "особой важности"

- указанным в п.1-3

10. Предельный срок пересмотра ранее установленных грифов секретности составляет

- 5 лет

- 1 год
- 10 лет
- 15 лет

7.2.3 Примерный перечень заданий для решения прикладных задач

1. Программное средство защиты информации

- криптография

- источник бесперебойного питания
- резервное копирование
- дублирование данных

2. Обеспечение достоверности и полноты информации и методов ее обработки

- конфиденциальность

- целостность

- доступность
- целесообразность

3. Как называется документ в программе MS Access?

- таблица

- база данных

- книга
- форма

4. Виды защиты БД

- защита паролем, защита пользователем

- учётная запись группы администратора
- приложение, которое используется для управления базой данных
- группа Users

5. Защита через права доступа заключается

- присвоении каждому пользователю определенного набора прав

- запереть серверы в специальном помещении с ограниченным доступом
- присвоить пароль каждому общедоступному ресурсу
- в наличии преобразователья микрофона

6. Наиболее распространенный криптографический код

- Код Хэмминга

- код Рида-Соломона
- код Морзе
- итеративный код

7. Функция технологии RAID 5

- дисковый массив повышенной производительности с чередованием, без отказоустойчивости
- зарезервирован для массивов, которые применяют код Хемминга

- хранит блок четности на одном физическом диске

- распределяет информацию о четности равномерно по всем дискам

8. Какой способ данные, дублируя и размещая их на различных физических носителях (например, на разных дисках)

- Журнал резервного копирования

- Отказоустойчивые системы

- Метод резервного копирования
- Шифрование данных

9. Международным стандартным кодом является

- Unicode

- CP866
- ASCII
- DOS
- Altair

10. Утилита Setup это - ?

- утилита входящая в состав BIOS

- утилита содержащее в себе BIOS
- BIOS не содержит ее
- настройка системы BIOS

7.2.4 Примерный перечень вопросов для подготовки к зачету

1. Дайте определение «информация», «защищаемая информация». Как классифицируется информация в зависимости от категории доступа, от порядка ее предоставления или распространения?

2. Дайте определение «защита информации». Что является предметом защиты?

3. Дайте определения: «угроза», «воздействие», «источник угроз», «уязвимость», «ущерб», «риск», «информационный риск».

4. Что такое «инцидент информационной безопасности» и «событие в системе информационной безопасности»?

5. Что представляет собой модель злоумышленника?

6. Что такое «защитная мера»? Какова структура защитных мер? Что относится к базовым защитным мерам?

7. Что представляет собой система обеспечения безопасности? Какие задачи она решает?

8. Дайте определение «информационная безопасность» и перечислите основные ее составляющие.

9. Перечислите и охарактеризуйте основные виды тайн.

10. Что представляет собой система менеджмента информационной безопасности? Перечислите и охарактеризуйте основные процессы, входящие в модель PDCA.

11. Что такое «политика информационной безопасности»? Перечислите основные ее положения.

12. Что понимается под национальной безопасностью РФ? Что относится к национальным интересам России в информационной сфере?

Приведите их классификацию, в соответствии с Доктриной информационной безопасности РФ.

13. Что понимается под информационной безопасностью РФ? Перечислите основные задачи обеспечения информационной безопасности РФ.

14. Перечислите виды угроз информационной безопасности РФ. Что относится к внешним и внутренним источникам угроз информационной безопасности РФ.

15. Что входит в общую структуру государственной системы обеспечения информационной безопасности РФ?

16. Перечислите основные функции и задачи, решаемые ФСТЭК России.

17. Какие задачи решает государственная система обеспечения информационной безопасности?

18. Перечислите основные принципы государственной политики обеспечения информационной безопасности РФ.

19. Перечислите основные мероприятия по реализации государственной политики обеспечения информационной безопасности РФ, определенные в Доктрине информационной безопасности РФ.

20. В чем заключается правовое обеспечение информационной безопасности? Что понимается под нормативно-правовым актом?

21. Опишите структуру нормативно-правового и справочного обеспечения информационной безопасности информационных технологий, охарактеризуйте отдельные компоненты.

22. Какие международные организации занимаются разработкой нормативно-правовых актов в области информационной безопасности.

23. Опишите основные концептуальные документы, определяющие основу защиты информации в России.

24. Перечислите основные федеральные законы РФ, определяющие систему защиты информации в России.

25. Какие вспомогательные нормативные акты регулируют процесс и механизмы исполнения положений и требований к системе обеспечения информационной безопасности государства? Дайте их краткую характеристику.

26. Как классифицируются информационные системы в зависимости от категории и объема обрабатываемых персональных данных?

27. Перечислите основные руководящие документы Гостехкомиссии России. Дайте их краткую характеристику.

28. Перечислите основные нормативно-методические документы ФСТЭК России в области защиты персональных данных. Дайте их краткую характеристику.

29. Перечислите основные руководящие документы ФСТЭК России по защите ключевых систем информационной инфраструктуры.

30. По каким параметрам могут классифицироваться угрозы информационной безопасности? Представьте системную классификацию угроз информационной безопасности и дайте их краткую характеристику.

31. Перечислите основные предпосылки появления угроз информационной безопасности, дайте их краткую характеристику.

32. Что понимается под источником угрозы информационной безопасности? Дайте их краткую характеристику.

33. Перечислите основные типы кибератак. Дайте их краткую характеристику.

34. Опишите основные составляющие модели угроз информационной безопасности.

35. Что такое каналы несанкционированного получения информации? На какие классы и по каким признакам они делятся?

36. По каким признакам классифицируются уязвимости информационной безопасности? Дайте их краткую характеристику.

37. Перечислите и охарактеризуйте основные методы оценки уязвимостей.

38. Какие выделяются категории стандартов по защите информации? Чем отличаются добровольные, регулирующие стандарты и регулятивное использование добровольных стандартов?

39. Перечислите наиболее известные зарубежные и отечественные стандарты в области информационной безопасности?

40. Что такое произвольное и принудительное управление доступом? Перечислите и охарактеризуйте основные элементы принудительного управления доступом.

41. По каким критериям классифицируются средства защиты данных? Что такое формальные и неформальные средства защиты?

42. Какие задачи решают, и по каким признакам классифицируются физические средства защиты информации?

43. Перечислите основные методы биометрической идентификации.

44. Что такое отказоустойчивые дисковые массивы (RAID)? Какие выделяют уровни RAID и какие принципы организации заложены в них?

45. Криптографические методы и средства защиты данных, основные понятия: криптография, открытый текст, шифрование данных, шифр, ключ, криптоанализ, криптология.

46. Классификация криптографических методов преобразования информации.

47. Отечественный стандарт на шифрование данных.

48. Современные симметричные системы шифрования.

49. Электронная цифровая подпись

50. Компьютерная стеганография.

51. Вредоносные программы и их классификация.

52. Методы обнаружения и удаления компьютерных вирусов.

53. Программные закладки и методы защиты от них.

54. Принципы построения систем защиты от копирования. Классификация.

55. Методы и средства защиты информации от несанкционированного доступа.

56. Аутентификация пользователей на основе паролей.

57. Аутентификация пользователей на основе модели «рукопожатия».

58. Аутентификация пользователей при удаленном доступе.

59. Межсетевые экраны.

60. Особенности удаления информации с электронных носителей. Политика уничтожения данных.

61. Следы в сети. Уникальные идентификаторы интернет-пользователей и электронные "отпечатки".

62. Обеспечение конфиденциальности в социальных сетях.

63. Методы проведения компьютерно-технической экспертизы.

64. Проведение расследования компьютерных инцидентов.

7.2.5 Примерный перечень заданий для решения прикладных задач

Не предусмотрено учебным планом

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

Зачет проводится по билетам, каждый из которых содержит 3 вопроса.

Первый вопрос оценивается на 1 балл, второй – на 2 балла, третий – на 3 балла. Максимальное количество набранных баллов – 6.

1. Оценка «Зачтено» ставится в случае, если студент набрал от 3 до 6 баллов.

2. Оценка «Не зачтено» ставится в случае, если студент набрал менее 3 баллов.

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Основные понятия и задачи информационной безопасности.	ОПК-1	Тест
2	Информационная безопасность Российской Федерации	ОПК-1	Тест
3	Международная, национальная и ведомственная нормативная правовая база в области информационной безопасности	ОПК-1	Тест, защита реферата
4	Безопасность (защищенность) компьютерных систем	ОПК-1	Тест, защита реферата
5	Вредоносное программное обеспечение	ОПК-1	Тест
6	Средства защиты и нападения	ОПК-1	Тест
7	Уничтожение информации	ОПК-1	Тест
8	Защита информации от утечки по техническим каналам	ОПК-1	Тест
9	Компьютерно-техническая экспертиза	ОПК-1	Тест

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.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Основная литература:

1. Чопоров, О.Н. Основы информационной безопасности [Электронный ресурс] . - Электрон. текстовые, граф. дан. (0,99 Мб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 30-00.

2. Нестеров, С. А. Основы информационной безопасности : учебник для вузов / С. А. Нестеров. — Санкт-Петербург : Лань, 2021. — 324 с. — ISBN 978-5-8114-6738-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/165837 (дата обращения: 28.02.2022). — Режим доступа: для авториз. пользователей.

Дополнительная литература:

1. Горбенко, А. О. Основы информационной безопасности : ведение в профессию : учебное пособие / А. О. Горбенко. — Санкт-Петербург : Интермедия, 2016. — 336 с. — ISBN 978-5-4383-0136-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/90265 (дата обращения: 28.02.2022). — Режим доступа: для авториз. пользователей.

2. Теория сетевых войн [Электронный ресурс] : Учеб. пособие. - Электрон. текстовые, граф. дан. (894 Мб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 30-00.

3. Методические указания к практическим занятиям по дисциплине

«Основы информационной безопасности» для студентов специальностей 090301 «Компьютерная безопасность», 090302 «Информационная безопасность телекоммуникационных систем», 090303 «Информационная безопасность автоматизированных систем» очной формы обучения [Электронный ресурс] / Каф. систем информационной безопасности; Сост.: О. Н. Чопоров, Н. Н. Корнеева. - Электрон. текстовые, граф. дан. (542 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2015. – 1 файл. - 00-00.

4. Методические указания к самостоятельным работам по дисциплине «Основы информационной безопасности» для студентов специальностей 090301 «Компьютерная безопасность», 090302 «Информационная безопасность телекоммуникационных систем», 090303 «Информационная безопасность автоматизированных систем» очной формы обучения [Электронный ресурс] / Каф. систем информационной безопасности; Сост. О. Н. Чопоров. - Электрон. текстовые, граф. дан. (348 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 00-00.

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:

Операционная система, не ниже Windows 7.

Пакет офисных программ, не ниже MS Office 2007.

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Для занятий необходимо наличие компьютерного класса с аудиовизуальной аппаратурой. Операционная система семейства Windows, не ниже Windows7, либо операционная система семейства AstraLinux актуальной версии. Антивирусный программный комплекс актуальной версии

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

По дисциплине «Основы информационной безопасности» читаются лекции, проводятся практические занятия.

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 практическое изучение рассматриваемых на лекциях методов и средств защиты информации и информационной безопасности. Занятия проводятся путем выступления студентов с рефератами, решения практических задач.

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.
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 зачетом три дня эффективнее всего использовать для повторения и систематизации материала.