МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Воронежский государственный технический университет»

УТВЕРЖДАЮ
Декан факультета экономики менеджмента и информационных технологий

_____ С.А.Баркалов

«30» августа 2017 г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«Защита компьютерной информации»

Направление подготовки 09.03.02 ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ

Профиль Информационные системы и технологии в строительстве

Квалификация выпускника Бакалавр
Нормативный период обучения 4 года
Форма обучения очная
Год начала подготовки 2017

Автор программы _____ /Маковий К.А./

Заведующий кафедрой Информационных технологий и автоматизированного проектирования в строительстве _____ /Смольянинов А.В./

Руководитель ОПОП _____ /Курипта О.В./

Воронеж 2017

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины

Целью дисциплины является изучение основополагающих принципов защиты информации на современных объектах информатизации. а также с нормативными правовыми актами Российской Федерации и зарубежных стран, регламентирующими деятельность в сфере защиты компьютерной информации.

1.2. Задачи освоения дисциплины

Задачами преподавания дисциплины являются:

- изучение нормативных правовых актов, регламентирующих деятельность в области защиты информации;
- изучение современных теоретических, практических и методологических аспектов защиты информации;
- изучение современных угроз информационной безопасности, а также концептуальных проблем выявления угроз информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Защита компьютерной информации» относится к дисциплинам вариативной части (дисциплина по выбору) блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Защита компьютерной информации» направлен на формирование следующих компетенций:

ОПК-1 - владение широкой общей подготовкой (базовыми знаниями) для решения практических задач в области информационных систем и технологий

ОПК-4 - пониманием сущности и значения информации в развитии современного общества, соблюдение основных требований к информационной безопасности, в том числе защиты государственной тайны

ПК-6 - способность оценивать надежность и качество функционирования объекта проектирования

ДПК-3 - способность обнаруживать угрозы безопасности и устранять нарушения целостности данных

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ОПК-1	Знать основные термины и определения в области защиты компьютерной информации
	Уметь структурировать информационные ресурсы в соответствии с их ценностью и уровнем конфиденциальности, определять необходимость

	их защиты от несанкционированного доступа
	Владеть методами построения защищенных информационных систем
ОПК-4	Знать правовые акты, затрагивающие вопросы обеспечения защиты компьютерной информации
	Уметь анализировать уровень эффективности используемых средств и методов защиты информации
	Владеть методами системного анализа информационных систем
ПК-6	Знать типы атак на информационные системы и методы борьбы с ними
	Уметь применять основополагающие принципы обеспечения информационной безопасности и защиты информации при проектировании информационных систем.
	Владеть навыком описания проектируемой системы с точки зрения обеспечения защиты компьютерной информации
ДПК-3	Знать основные аспекты защиты информации
	Уметь обнаруживать угрозы безопасности
	Владеть навыком проверки целостности данных

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Защита компьютерной информации» составляет 3 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры
		5
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 з.е.	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	Основы информационной безопасности и защиты информации в современных условия	Нормативные правовые акты регламентирующие деятельность в сфере обеспечения информационной безопасности и защиты информации. Основные термины и определения информационной безопасности и защиты информации. Исторические аспекты развития информационной безопасности как науки. Проблема обеспечения информационной безопасности в Российской Федерации. Требования к защите конфиденциальной и секретной информации. Информационная безопасность как неотъемлемая часть деятельности общества. Классификация современных методов обеспечения информационной безопасности. Системный подход в вопросе обеспечения информационной безопасности и защиты информации на объектах информатизации. Побочные электромагнитные излучения	4	2	12	18

		и наводки как канал утечки защищаемой информации.				
2	Методы и средства обеспечения информационной безопасности.	Современные системы разграничения доступа к информационным ресурсам. Использование организационно-правовых, технических (аппаратных), программных, программно-аппаратных методов защиты информации. Задачи систем обеспечения информационной безопасности. Разграничение доступа как средство обеспечения защиты информации. Модели разграничения доступа, разделение привилегий на доступ.	4	2	12	18
3	Криптографические средства обеспечения информационной безопасности	Шифрование как инструмент защиты информации. Криптографические методы и средства обеспечения защиты информации. Использование криптографических средств защиты информации в современных информационных системах.	4	2	12	18
4	Вредоносное программное обеспечение как угроза информационной безопасности.	Исторические аспекты компьютерных вирусов. Компьютерные вирусы как разновидность вредоносного программного обеспечения в современных условиях. Классификация компьютерных вирусов. Интеграция вредоносного программного обеспечения в мобильных платформах. Методы и способы обнаружения и анализа	2	4	12	18

		алгоритма вредоносного программного обеспечения.				
5	Реализация мер защиты информации на программном уровне.	Реализация механизмов защиты информации как компонент современных информационных систем. Правовые основы использования механизмов защиты информации в современных информационных системах. Исследование программного обеспечения как угроза информационной безопасности. Методы и средства защиты программного обеспечения от исследование. Роль механизмов идентификации и аутентификации в современном программном обеспечении.	2	4	12	18
6	Вопросы обеспечения защиты информации в распределенных информационных системах.	Особенности формирования каналов утечки информации в распределенных информационных системах. Современные средства и методы анализа состояния защищенности распределенных информационных систем. Проблемы обеспечения информационной безопасности в современных распределенных информационных системах. Аспекты разработки модели угроз распределенной информационной системы.	2	4	12	18
		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».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ОПК-1	Знать основные термины и определения в области защиты компьютерной информации	Активное участие в устных опросах на занятиях, готовит доклады и рефераты по изучаемым темам	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь структурировать информационные ресурсы в соответствии с их ценностью и уровнем конфиденциальности, определять необходимость их защиты от несанкционированного доступа	Выполнение практических заданий	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть методами построения защищенных информационных систем	Выполнение практических заданий	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ОПК-4	Знать правовые акты, затрагивающие вопросы обеспечения защиты компьютерной информации	Активное участие в устных опросах на занятиях, готовит доклады и рефераты по изучаемым темам	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь анализировать уровень эффективности используемых средств и методов защиты информации	Выполнение практических заданий	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть методами системного анализа информационных	Выполнение практических заданий	Выполнение работ в срок, предусмотренный в	Невыполнение работ в срок, предусмотренный

	систем		рабочих программах	в рабочих программах
ПК-6	Знать типы атак на информационные системы и методы борьбы с ними	Активное участие в устных опросах на занятиях, готовит доклады и рефераты по изучаемым темам	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь применять основополагающие принципы обеспечения информационной безопасности и защиты информации при проектировании информационных систем.	Выполнение практических заданий	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть навыком описания проектируемой системы с точки зрения обеспечения защиты компьютерной информации	Выполнение практических заданий	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ДПК-3	Знать основные аспекты защиты информации	Активное участие в устных опросах на занятиях, готовит доклады и рефераты по изучаемым темам	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь обнаруживать угрозы безопасности	Выполнение практических заданий	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть навыком проверки целостности данных	Выполнение практических заданий	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 5 семестре для очной формы обучения по двухбалльной системе:

«зачтено»

«не зачтено»

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Зачтено	Не зачтено
ОПК-1	Знать основные термины и определения в области защиты компьютерной информации	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	Уметь структурировать информационные ресурсы в соответствии с их ценностью и уровнем конфиденциальности, определять	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены

	необходимость их защиты от несанкционированного доступа			
	Владеть методами построения защищенных информационных систем	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
ОПК-4	Знать правовые акты, затрагивающие вопросы обеспечения защиты компьютерной информации	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	Уметь анализировать уровень эффективности используемых средств и методов защиты информации	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
	Владеть методами системного анализа информационных систем	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
ПК-6	Знать типы атак на информационные системы и методы борьбы с ними	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	Уметь применять основополагающие принципы обеспечения информационной безопасности и защиты информации при проектировании информационных систем.	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
	Владеть навыком описания проектируемой системы с точки зрения обеспечения защиты компьютерной информации	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
ДПК-3	Знать основные аспекты защиты информации	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	Уметь обнаруживать угрозы безопасности	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
	Владеть навыком проверки целостности данных	Решение прикладных задач в конкретной предметной области	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

Таблица 1

Значение термина "Защита информации" определено в Федеральном законе:
Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации"
Федеральный закон от 27 июля 2006 г. N **152-ФЗ** "О персональных данных"
Федеральный закон от 27 июля 2006 г. N 159-ФЗ "О защите информации в Российской Федерации"

Таблица 2

Информация – это
сведения (сообщения, данные) независимо от формы их представления
Любые сведения обрабатываемые в информационных системах
Данные об объектах, лицах, независимо от формы их представления.
Персональные данные не зависимо от формы представления.

Таблица3

Авторизация – это:
Предоставление конкретному пользователю к определенным системным ресурсам
Проверка личности пользователя
Идентификация пользователя
Аутентификация пользователя

Таблица 4

К числу основных угроз информационной безопасности не относится:
Защита от копирования
Целостность
Доступность
Конфиденциальность

Таблица 5

Политика информационной безопасности строится на основе:
Анализа рисков
Сбора сведений о персонале
Общих представлений об АИС объекта информатизации
Изучения номенклатуры должностей организации

Таблица 6

Технологическая система, предназначенная для передачи по линиям связи информаци доступ к которой осуществляется с использованием средств вычислительной техники это
Информационно-телекоммуникационная сеть
Информационная система
База данных
Информационная технология

Таблица 7

Компоненты информационной системы предприятия, в котором накапливаются обрабатываются персональные данные это:
Информационная сеть персональных данных
Система управления базами данных
Хранилище данных
Коммуникационный узел

Таблица 8

Процесс сообщения субъектом своего имени или номера, с целью получения определенны полномочий на выполнение некоторых действий в информационных системах ограниченным доступом:
Идентификация

Авторизация
Регистрация
Детализация

Таблица 9

Основное средство, обеспечивающее конфиденциальность информации, посылаемой по открытым каналам передачи информации, в том числе по сети Интернет:
Шифрования
Парольная защита
Авторизация пользователей сети
Экспертиза

Таблица 10

Несанкционированный доступ к информации – это:
Доступ к информации, не связанный с выполнением функциональных обязанностей и не оформленный документально
Вход в информационную систему без регистрации пользователя
Доступ к информационным ресурсам от имени другого пользователя
Доступ к информационным ресурсам, связанный с выполнением функциональных обязанностей

7.2.2 Примерный перечень заданий для решения стандартных задач

Таблица 11

Может ли сотрудник быть привлечен к уголовной ответственности за нарушения правил информационной безопасности организации:
Да
Нет
Нет, если это государственная организация
Да, если это государственная организация

Таблица 12

Пароль пользователя должен:
Содержать цифры и буквы разного регистра, знаки препинания, быть сложным для угадывания
Содержать только цифры
Содержать только буквы
Иметь привязку к пользователю

Таблица 13

Хищение информации - это:
Несанкционированное копирование информации
Утрата информации
Продажа информации
Приобретение информации

Таблица 14

Владельцем информации составляющей государственную тайну является:
Государство
Правительство Российской Федерации
Граждане
Президент

Таблица 15

Электронные замки "Соболь" предназначены для:
Обеспечения доверенной загрузки компьютера и контроля целостности файлов в системах
Сканирования системы
Регистрации входа пользователей

Идентификации пользователей

Таблица 16

Информация об уголовной ответственности за преступления в сфере компьютерн информации описана:
28 главе Уголовного Кодекса
1 главе Уголовного Кодекса
в собрании уголовного законодательства Российской Федерации
в Уголовном Кодексе данный вопрос не регламентирован

7.2.3 Примерный перечень заданий для решения прикладных задач

1. Проанализировать разделы, структуру в целом, физического диска персонального компьютера.

2. Произвести разграничение доступа к локальным и сетевым ресурсам, провести аудит системы безопасности стандартными средствами операционной системы семейства Windows.

3. Использование возможностей защиты документа, а также ЭЦП при работе с текстовым редактором Microsoft Word.

4. Использование возможностей защиты документа, а также ЭЦП при работе с табличным редактором Microsoft Excel.

5. Создание архивов данных с использованием парольной защиты, исследование парольной защиты программных архиваторов RAR, ZIP, ARJ.

6. Восстановление информации на носителей информации.

7. Обнаружение и удаление компьютерных вирусов средствами антивирусной защиты информации.

8. Анализ угроз информационной безопасности на объектах информатизации использующих информационные системы обработки персональных данных.

9. Обзор методов криптографии. Шифрование и дешифрование данных криптографическими методами преобразования.

7.2.4 Примерный перечень вопросов для подготовки к зачету

1. Национальные интересы Российской Федерации в области информацион-ной безопасности.

2. Основные угрозы безопасности. Информационная безопасность. Опреде-ление. Аспекты информационной безопасности. Направления обеспечения ИБ

3. Жизненно важные интересы и угрозы в информационной сфере. Уровни угроз ИБ и их классификация.

4. Отечественные и зарубежные стандарты в области информационной без-опасности.

5. Защита информации. Определение. Формы и способы защиты. Политика безопасности и гарантированности.

6. Основные предметные направления защиты информации. Правовые осно-вы защиты информации. Структура законодательства России в области защиты информации.

7. Источники права на доступ к информации. Информация как объект соб-ственности: право владения, право пользования и право распоряжения.

Федеральный Закон «Об информации, информатизации и защите инфор-мации».

8. Уровни доступа к информации с точки зрения законодательства. Виды до-ступа и механизмы доступа к информации.

9. Ответственность за нарушение законодательства в информационной сфере. Формы защиты права на доступ к информации.

10. Предмет и объекты защиты информации в автоматизированных системах обработки информации (АСОД). Надежность информации. Уязвимость информации.

11. Элементы и объекты защиты в АСОД. Основные элементы АСОД и типо-вые структурные компоненты.

12. Дестабилизирующие факторы АСОД. Причины нарушения целостности информации. Каналы несанкционированного получения информации в АСОД.

13. Преднамеренные угрозы безопасности АСОД. Атаки. Классификация угроз безопасности.

14. Функции и задачи защиты информации в АСОД. Механизм защиты.

15. Методы и системы защиты информации в АСОД. Целостность и конфи-денциальность информации.

16.Аутентификация и идентификация. Подтверждение подлинности пользова-телей и разграничение их доступа к компьютерным ресурсам. Контроль доступа к аппаратуре.

17. Процедура опознавания с использование простого пароля. Методы про-верки подлинности на основе динамически изменяющегося пароля.

18. Методы идентификации и установления подлинности субъектов и различ-ных объектов. Функциональные методы.

19. Контроль информационной целостности. Организация контроля. Спосо-бы модификаций информации.

20. Защита информации от утечки по техническим каналам. Определения, понятия и виды каналов утечки.

21. Защита информации от утечки по визуально-оптическим и акустическим каналам.

22. Защита информации от утечки по электромагнитным и материально-вещественным каналам.

23. Технические средства защиты. Классификация технических средств. Функции защиты и степень сложности устройства.

24. Механические системы защиты. Системы оповещения. Системы опознава-ния. Оборонительные системы. Охранное освещение.

25. Физические средства защиты. Средства контроля доступа. Автоматизиро-ванные системы контроля доступа.

26. Биометрические системы идентификации. Основные методы. Охранные системы.

7.2.5 Примерный перечень вопросов к экзамену

Не предусмотрено учебным планом

7.2.6. Методика выставления оценки при проведении

промежуточной аттестации

Зачет проводится по тест-билетам, каждый из которых содержит 10 вопросов и задачу. Каждый правильный ответ на вопрос в тесте оценивается 1 баллом, задача оценивается в 10 баллов (5 баллов верное решение и 5 баллов за верный ответ). Максимальное количество набранных баллов – 20.

1. Оценка «незачтено» ставится в случае, если студент набрал менее 86 баллов.

2. Оценка «Зачтено» ставится в случае, если студент набрал от 8 до 20 баллов

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Основы информационной безопасности и защиты информации в современных условия	ОПК-1, ОПК-4, ПК -6, ДПК-3	Тест, защита реферата, выполнение практических заданий
2	Методы и средства обеспечения информационной безопасности.	ОПК-1, ОПК-4, ПК -6, ДПК-3	Тест, защита реферата, выполнение практических заданий
3	Криптографические средства обеспечения информационной безопасности	ОПК-1, ОПК-4, ПК -6, ДПК-3	Тест, защита реферата, выполнение практических заданий
4	Вредоносное программное обеспечение как угроза информационной безопасности.	ОПК-1, ОПК-4, ПК -6, ДПК-3	Тест, защита реферата, выполнение практических заданий
5	Реализация мер защиты информации на программном уровне.	ОПК-1, ОПК-4, ПК -6, ДПК-3	Тест, защита реферата, выполнение практических заданий
6	Вопросы обеспечения защиты информации в распределенных информационных системах.	ОПК-1, ОПК-4, ПК -6, ДПК-3	Тест, защита реферата, выполнение практических заданий

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

1. Артемов А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ Артемов А.В.— Электрон. текстовые данные.— Орел: Межрегиональ-ная Академия безопасности и выживания (МАБИВ), 2014.— 256 c.— Режим доступа: http://www.iprbookshop.ru/33430.— ЭБС «IPRbooks», по паролю

2. Галатенко В.А. Основы информационной безопасности [Электронный ресурс] / В.А. Галатенко. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 266 c. — 978-5-94774-821-5. — Режим доступа: http://www.iprbookshop.ru/52209.html

3. Авдошин С.М. Технологии и продукты Microsoft в обеспечении информацион-ной безопасности [Электронный ресурс] / С.М. Авдошин, А.А. Савельева, В.А. Сердюк. — Электрон. текстовые данные. — Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образова-ние, 2017. — 412 c. — 978-5-4487-0147-4. — Режим доступа: http://www.iprbookshop.ru/72341.html

4. Басалова Г.В. Основы криптографии [Электронный ресурс] / Г.В. Басалова. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 282 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/52158.html

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 Windows 7, Windows 2008 Server, Linux Mint 19.1;
- интернет браузеры: Yandex Browser, Google Chrome и другие;
- Oracle Virtual Box

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

1. *Технические средства:*
a. *Компьютерный класс с выходом в Интернет.*
b. *На каждом рабочем месте – ПО Oracle Virtual Box.*
c. *Проектор.*
2. *Программное обеспечение:*
a. *Интернет браузеры: Yandex-Browser, Google Chrome и другие*
b. *Программа Microsoft Word – текстовый редактор.*
c. *Программа Adobe Acrobat Reader – средство чтения электрон-ных материалов в формате PDF.*
d. *Программа MS EXEL –электронные таблицы*

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

По дисциплине «Защита компьютерной информации» проводятся лекции и 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 приобретение практических навыков определения угроз защиты информации. Занятия проводятся путем решения конкретных задач в компьютерных классах, оснащенных возможностью установки виртуальных операционных систем

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.