АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
«ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ»
«УНИВЕРСИТЕТ ЭКОНОМИКИ И УПРАВЛЕНИЯ»
Факультет экономики и управления
Кафедра «Бизнес-информатика»

УТВЕРЖДАЮ
Проректор по учебно-
методической работе
_____ С.С. Скараник
«01» сентября 2020 г.

Рабочая программа дисциплины
Информационная безопасность

Направление подготовки
38.04.09 Государственный аудит

Квалификация выпускника
Магистр

Для всех
форм обучения

Симферополь 2020

Содержание

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

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

Коды компетенции	Результаты освоения ОПОП	Перечень планируемых результатов по дисциплине
ОПК-2	способностью использовать в познавательной и профессиональной деятельности базовые знания в области основ информатики и элементы естественно-научного и математического знания	**Знать:** - базовые знания в области основ информатики и элементы естественнонаучного и математического знания; - тематические сетевые ресурсы, базы данных, информационно-поисковые системы; - методы использования в исследова-ниях тематические сетевые ресурсы, базы данных, информационно-поисковые системы; - методы использования баз данных и информационных систем при реализации организационно-управленческих функций; **Уметь:** - использовать в познавательной и профессиональной деятельности базовые знания в области основ информатики и элементы естественно-научного и математического знания; - использовать в исследованиях тематические сетевые ресурсы, базы данных, информационно-поисковые системы; - использовать базы данных и информационные системы при реализации организационно-управленческих функций; **Владеть:** - способностью использовать в познавательной и профессиональной деятельности базовые знания в области основ информатики и элементы естественнонаучного и математическо-го знания; - способностью использовать в исследованиях тематические сетевые ресурсы, базы данных, информационно-поисковые системы; - способностью к использованию баз данных и информационных систем при реализации организационно-управленческих функций
ПК-4	способностью использовать в исследованиях тематические сетевые ресурсы, базы данных, информационно-поисковые системы	
ПК-12	способностью к использованию баз данных и информационных систем при реализации организационно-управленческих функций	

2. Место дисциплины в структуре ОПОП ВО

Дисциплина Б1.В.ДВ.01.01 «Информационная безопасность» входит в вариативную часть.

Дисциплина основывается на знании следующих дисциплин: «Информационные технологии в экономических и правовых исследованиях и образовании», «Информатика».

3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 2 зачетных единицы, 72 академических часов.

Объём дисциплины по видам учебных занятий (в часах)

Для очной формы обучения

Общая трудоёмкость дисциплины составляет 2 зачётных единицы 72 часов

Объём дисциплины	Всего часов
Общая трудоемкость дисциплины	72
Контактная работа	32
Аудиторная работа (всего):	28
Лекции	12
Семинары, практические занятия	16
Внеаудиторная работа (всего):	
Самостоятельная работа обучающихся	40
Зачет	4

Для заочной формы обучения

Общая трудоёмкость дисциплины составляет 2 зачётных единицы 72 часов

Объём дисциплины	Всего часов
Общая трудоемкость дисциплины	72
Контактная работа	10
Аудиторная работа (всего):	6
Лекции	2
Семинары, практические занятия	4
Внеаудиторная работа (всего):	
Самостоятельная работа обучающихся	62
Зачет	4

4. Содержание дисциплины, структурированное по темам с указанием отведенного на них количества академических часов и видов учебных занятий

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

№ п/п	Наименование темы	Всего		Количество часов					
		ОФО	ЗФО	Контактная работа (Аудиторная работа)				Внеаудит. работа	
				Лекции		Практические		Самост. работа	
				ОФО	ЗФО	ОФО	ЗФО	ОФО	ЗФО
1	2	3	4	5	6	7	8	10	11
1	Тема 1. Общие вопросы информационной безопасности	8	6,5	2	0,5	2		4	6
2	Тема 2. Государственная система информационной безопасности	8	7,5	1	0,5	1	1	6	6
3	Тема 3. Угрозы безопасности	8	7,5	1	0,5	1	1	6	6
4	Тема 4. Теоретические основы методов защиты информационных систем	8	7	2		2		4	7
5	Тема 5. Методы защиты средств вычислительной техники	8	8	2		2		4	8
6	Тема 6. Основы криптографии	8	8	2		2	1	4	7
7	Тема 7. Архитектура защищенных экономических систем	7	8	1		2		4	8
8	Тема 8. Алгоритмы привязки программного обеспечения к аппаратному окружению	7	8	1		2		4	8
9	Тема 9. Алгоритмы безопасности в компьютерных сетях	6	7,5		0,5	2	1	4	6
	Всего по дисциплине	68	68	12	2	16	4	40	62
	Зачет	4	4						
	Итого	**72**	**72**	**12**	**2**	**16**	**4**	**40**	**62**

4.2 Содержание дисциплины, структурированное по темам (разделам)

Тема 1. Общие вопросы информационной безопасности

Основные понятия и определения. Понятия информация, информатизация, информационная система, информационная безопасность. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене. Защита информации, тайна, средства защиты информации. Международные стандарты информационного обмена. Показатели информации: важность, полнота, адекватность, релевантность, толерантность. Требования к защите информации. Комплексность системы защиты информации: инструментальная, структурная, функциональная, временная.

Тема 2. Государственная система информационной безопасности

Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Доктрина информационной безопасности Российской Федерации. Структура государственной системы информационной безопасности. Структура законодательной базы по вопросам информационной безопасности. Лицензирование и сертификация в области защиты информации. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.

Тема 3. Угрозы безопасности

Понятие угрозы. Виды противников или «нарушителей». Классификация угроз информационной безопасности. Виды угроз. Основные нарушения. Характер происхождения угроз (умышленные и естественные факторы). Источники угроз. Предпосылки появления угроз. Классы каналов несанкционированного получения информации. Причины нарушения целостности информации.

Тема 4. Теоретические основы методов защиты информационных систем

Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Формальные модели безопасности. Дискреционная модель Харрисона-Руззо-Ульмана. Типизированная матрица доступа. Модель распространения прав доступа Take-Grant. Мандатная модель Белла-Ла-Падулы. Ролевая политика безопасности. Ограничения на области применения формальных моделей.

Тема 5. Методы защиты средств вычислительной техники

Использование защищенных компьютерных систем. Аппаратные и программные средства для защиты компьютерных систем от НСД. Средства операционной системы. Средства резервирования данных. Проверка целостности. Способы и средства восстановления работоспособности.

Тема 6. Основы криптографии

Методы криптографии. Симметричное и асимметричное шифрование. Алгоритмы шифрования. Электронно-цифровая подпись. Алгоритмы электронно-цифровой подписи. Хеширование. Имитовставки. Криптографические генераторы случайных чисел. Способы распространения ключей. Обеспечиваемая шифром степень защиты. Криптоанализ и атаки на криптосистемы. Сжатие информации.

Тема 7. Архитектура защищенных экономических систем

Основные технологии построения защищенных экономических информационных систем. Функции защиты информации. Классы задач защиты информации. Архитектура систем защиты информации. Ядро и ресурсы

средств защиты информации. Стратегии защиты информации. Особенности экономических информационных систем.

Тема 8. Алгоритмы привязки программного обеспечения к аппаратному окружению

Индивидуальные параметры вычислительной системы. Блок проверки аппаратного окружения. Дискета как средство привязки. Технология HASP, эмуляторы. Временные метки и запись в реестр. Обеспечение требуемого количества запусков (trial version). Технология spyware. Виды распространения программного обеспечения. Шифрование и запутывание исполняемого кода.

Тема 9. Алгоритмы безопасности в компьютерных сетях

Межсетевые экраны. Проектирование МЭ. Снифферы. Эксплоиты. Атаки на сервера. Атаки на рабочие станции. Атака типа «отказ в обслуживании». Протоколирование. Сетевые защищенные протоколы.

4.3. Темы практических занятий

Практическая работа № 1. Понятия информация, информатизация, информационная система, информационная безопасность. Идентификация и аутентификация пользователя.

Практическая работа № 2. Электронно-цифровая подпись и приемы хеширования. Пакеты антивирусных программ.

Практическая работа № 3 Защита информации от копирования

Практическая работа № 4 Основные методы и приемы защиты от несанкционированного доступа

Практическая работа № 5 Шифрование методом перестановки

Практическая работа № 6 Защита программ в оперативной памяти. Приемы работы с защищенными программами.

Практическая работа № 7 Алгоритмы привязки программного обеспечения к аппаратному окружению

Практическая работа № 8 Перехват вывода на экран, перехват ввода с клавиатуры. Перехват и обработка файловых операций

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Тема (разделы)	Содержание заданий, выносимых на СРС	Кол-во часов ОФО	Кол-во часов ЗФО	Учебно-методическое обеспечение
1.	Тема 1. Общие вопросы информационной безопасности	4	6	Учебно-методическое пособие
2.	Тема 2. Государственная система информационной безопасности	6	6	Учебно-методическое пособие
3.	Тема 3. Угрозы безопасности	6	6	Учебно-методическое пособие
4.	Тема 4. Теоретические основы методов защиты	4	7	Учебно-методическое пособие

Тема (разделы)	Содержание заданий, выносимых на СРС	Кол-во часов ОФО	Кол-во часов ЗФО	Учебно-методическое обеспечение
	информационных систем			
5.	Тема 5. Методы защиты средств вычислительной техники	4	8	Учебно-методическое пособие
6.	Тема 6. Основы криптографии	4	7	Учебно-методическое пособие
7.	Тема 7. Архитектура защищенных экономических систем	4	8	Учебно-методическое пособием
8.	Тема 8. Алгоритмы привязки программного обеспечения к аппаратному окружению	4	8	Учебно-методическое пособие
9.	Тема 9. Алгоритмы безопасности в компьютерных сетях	4	6	Учебно-методическое пособие

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

6.1 Паспорт фонда оценочных средств по дисциплине

Компетенция ОПК-2

способностью использовать в познавательной и профессиональной деятельности базовые знания в области основ информатики и элементы естественнонаучного и математического знания		
Этапы формирования компетенции		
Знает	Умеет	Владеет
- базовые знания в области основ информатики и элементы естественнонаучного и математического знания. 6.2.1 (1-50)	- использовать в познавательной и профессиональной деятельности базовые знания в области основ информатики и элементы естественно-научного и математического знания. 6.2.2 (1-22) 6.2.3 (1-20)	- способностью использовать в познавательной и профессиональной деятельности базовые знания в области основ информатики и элементы естественнонаучного и математического знания. 6.2.4 (1-5)
Показатели и критерии оценивания компетенции на различных этапах ее формирования, шкала оценивания		
Знает, если выполнил 6.2.1 (1-50) Умеет, если выполнил 6.2.2 (1-22), 6.2.3 (1-20) Владеет, если выполнил 6.2.4 (1-5)		

Компетенция ПК-4

способностью использовать в исследованиях тематические сетевые ресурсы, базы данных, информационно-поисковые системы.		
Этапы формирования компетенции		
Знает	Умеет	Владеет
- тематические сетевые ресурсы, базы данных, информационно-поисковые системы. 6.2.1 (1-50)	- использовать в исследованиях тематические сетевые ресурсы, базы данных, информационно-поисковые системы. 6.2.2 (1-22) 6.2.3 (1-20)	- способностью использовать в исследованиях тематические сетевые ресурсы, базы данных, информационно-поисковые системы. 6.2.4 (1-5)
Показатели и критерии оценивания компетенции на различных этапах ее формирования, шкала оценивания		
Знает, если выполнил 6.2.1 (1-50) Умеет, если выполнил 6.2.2 (1-22), 6.2.3 (1-20) Владеет, если выполнил 6.2.4 (1-5)		

Компетенция ПК-12

способностью к использованию баз данных и информационных систем при реализации организационно-управленческих функций		
Этапы формирования компетенции		
Знает	Умеет	Владеет
- методы использования баз данных и информационных систем при реализации организационно-управленческих функций. 6.2.1 (1-50)	- использовать базы данных и информационные системы при реализации организационно-управленческих функций. 6.2.2 (1-22) 6.2.3 (1-20)	- способностью к использованию баз данных и информационных систем при реализации организационно-управленческих функций. 6.2.4 (1-5)
Показатели и критерии оценивания компетенции на различных этапах ее формирования, шкала оценивания		
Знает, если выполнил 6.2.1 (1-50) Умеет, если выполнил 6.2.2 (1-22), 6.2.3 (1-20) Владеет, если выполнил 6.2.4 (1-5)		

6.2 Типовые контрольные задания или иные материалы

6.2.1. Типовые вопросы на зачет:

1. Особенности современных автоматизированных систем.
2. Требования к системам и средствам защиты информации от несанкционированного доступа.
3. Показатели защищенности средств вычислительной техники.
4. Соответствие классов систем различным уровням конфиденциальности.
5. Понятие модели нарушителя информационной безопасности и модели угроз информационной безопасности.
6. Принципы построения системы защиты информации.

7. Определение уязвимостей автоматизированных систем и выбор средств защиты.
8. Классификация каналов утечки информации.
9. Методы защиты речевой информации.
10. Инженерно-техническая защита информации.
11. Методы противодействия разведкам.
12. Методы контроля доступа к ресурсам компьютерной системы.
13. Модели безопасности компьютерных систем.
14. Методы поиска остаточной информации на машинных носителях.
15. Методы гарантированного удаления информации.
16. Сущность разрушающих программных воздействий.
17. Модели взаимодействия прикладных программ и программы-злоумышленника, классификация разрушающих программных средств.
18. Компьютерные вирусы. Принципы и методы защиты от разрушающих программных воздействий.
19. Уязвимости приложений: атаки типа переполнение буфера, стека и кучи, атаки, основанные на изменении входных данных.
20. Требования ФСТЭК России к программному обеспечению средств защиты и его классификация по уровню отсутствия недекларированных возможностей.
21. Современная доктрина информационной безопасности Российской Федерации.
22. Государственная, общественная и социальная информационная безопасность.
23. Информационные войны и информационное оружие.
24. Киберпреступность в глобальной информационной сети.
25. Правовое обеспечение информационной безопасности. Организационное обеспечение информационной безопасности.
26. Технические методы и средства защиты информации. Программно-аппаратные средства информационной безопасности.
27. Криптографические методы защиты информации. Комплексное обеспечение информационной безопасности.
28. Системы и сети передачи информации.
29. Безопасность вычислительных систем.
30. Безопасность каналов передачи данных.

6.2.2. Темы рефератов или сообщений:

1. Этапы и общие принципы разработки защищенных информационных систем.
2. Предпосылки отнесения информации к категории конфиденциальной и выявление конфиденциальных сведений.
3. Сценарии последовательности действий нарушителя системы защиты информации. Пример построения сценария действий нарушителя с использованием графов.
4. Международные стандарты в области защиты информационных систем.

5. Цели, задачи и стадии проведения аудита информационной безопасности.

6. Оценка ущерба от нарушений информационной безопасности на различных этапах жизненного цикла объекта информатизации.

7. Методы оценки рисков информационной безопасности.

8. Шкалы оценки ущерба при нарушении информационной безопасности на объекте оценки.

9. Управление рисками. Модель безопасности с полным перекрытием.

10. Концепция управление рисками согласно ISO-15408.

11. Lifecycle Security – обобщенная схема построения комплексной защиты компьютерной сети предприятия.

12. Методика управления рисками, предлагаемая Microsoft (MSAT).

13. Обзор современных программных продуктов для оценки рисков.

14. Особенности моделирования сложных организационно-технических систем.

15. Моделирование процесса защиты информации в информационной системе с использованием графовых структур.

16. Пример использования графов для расчета защищенности от физического проникновения.

17. Генерирование множества альтернатив с применением экспертных методов при построении защищенной системы обработки информации.

18. Модель процесса защиты информации в виде трёхдольного графа.

19. Оценка альтернативных проектов организации системы защиты информации с использованием критериального метода.

20. Оценка альтернативных проектов организации системы защиты информации с использованием метода парных сравнений.

21. Информационные технологии, используемые в системах поддержки управленческих решений в области построения защищенных систем обработки информации.

22. Перспективные направления в организации и управлении системой защиты информации на предприятии.

6.2.3. Типовые вопросы теста

1. Под информационной безопасностью понимается…

А) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре.

Б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия

В) нет правильного ответа

2. Защита информации – это..

А) процесс разработки структуры базы данных в соответствии с требованиями пользователей

Б) комплекс мероприятий, направленных на обеспечение информационной безопасности.

В) небольшая программа для выполнения определенной задачи

3. От чего зависит информационная безопасность?

А) от информации

Б) от поддерживающей инфраструктуры

В) от компьютеров

4. Основные составляющие информационной безопасности:

А) целостность

Б) достоверность

В) конфиденциальность

5. Конфиденциальность – это..

А) защита от несанкционированного доступа к информации

Б) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов

В) описание процедур

6. Для чего создаются информационные системы?

А) обработки информации

Б) получения определенных информационных услуг

В) все ответы правильные

7. Какие трудности возникают в информационных системах при конфиденциальности?

А) сведения о технических каналах утечки информации являются закрытыми

Б) на пути пользовательской криптографии стоят многочисленные технические проблемы

В) все ответы правильные

8. Угроза – это…

А) потенциальная возможность определенным образом нарушить информационную безопасность

Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных

В) процесс определения отвечает на текущее состояние разработки требованиям данного этапа

9. Атака – это…

А) потенциальная возможность определенным образом нарушить информационную безопасность

Б) попытка реализации угрозы

) программы, предназначенные для поиска необходимых программ.

10. Источник угрозы – это..

А) потенциальный злоумышленник

Б) злоумышленник

В) нет правильного ответа

11. Угрозы можно классифицировать по нескольким критериям:

А) по спектру И.Б.

Б) по способу осуществления

В) по компонентам И.С.

12. По каким компонентам классифицируется угрозы доступности:

А) отказ пользователей

Б) отказ поддерживающей инфраструктуры

В) ошибка в программе

13. Основными источниками внутренних отказов являются:

А) отступление от установленных правил эксплуатации

Б) разрушение данных

В) все ответы правильные

14. По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:

А) невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности

Б) обрабатывать большой объем программной информации

В) нет правильного ответа

15. Вирус – это…

А) небольшая программа для выполнения определенной задачи

Б) способность объекта реагировать на запрос сообразно своему типу, при этом одно и то же имя метода может использоваться для различных классов объектов

В) код обладающий способностью к распространению путем внедрения в другие программы

16. Конфиденциальную информацию можно разделить:

А) предметную

Б) служебную

В) глобальную

17. Предпосылки появления угроз:

А) преднамеренные

Б) субъективные

В) объективные

18. К какому виду угроз относится присвоение чужого права?

А) нарушение права собственности

Б) нарушение содержания

В) внешняя среда

19. Отказ, ошибки, сбой – это:

А) природные угрозы

Б) преднамеренные угрозы

В) случайные угрозы

20. Отказ - это…

А) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций

Б) некоторая последовательность действий, необходимых для выполнения конкретного задания

В) структура, определяющая последовательность выполнения и взаимосвязи процессов

21) Хранение паролей может осуществляться

А. в виде сверток

Б. в открытом виде

В. в закрытом виде

Г. в зашифрованном виде

Д. все варианты ответа верны

22) К системам оповещения относятся:

А. инфракрасные датчики

Б. электрические датчики

В. электромеханические датчики

Г. электрохимические датчики

23) Злонамеренные действия в нематериальной сфере могут быть подразделены на два класса, какие?

А. Информационный саботаж

Б. Физический саботаж

В. Информационные инфекции

24) Что не относится к информационной инфекции:

А. Троянский конь

Б. Фальсификация данных

В. Черви

Г. Вирусы

Д. Логическая бомба

25) Деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения и несанкционированного доступа к защищаемой информации и от получения защищаемой информации:

А. защита информации от непреднамеренного воздействия
Б. защита информации от несанкционированного воздействия
В. защита информации от несанкционированного доступа
Г. защита от утечки информации

26) Исследование возможности дешифрования информации без знания ключей:

А. криптология
Б. криптоанализ
В. взлом
Г. несанкционированный доступ

27) Информация, не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения, в преимущественное положение по сравнению с другими объектами:

А. Служебная информация
Б. Коммерческая тайна
В. Банковская тайна
Г. Конфиденциальная информация

28**) Действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости системы.**

А. Комплексное обеспечение информационной безопасности
Б. Безопасность АС
В. Угроза информационной безопасности
Г. Атака на автоматизированную систему
Д. Политика безопасности

29) Набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных:

А. Защита информации
Б. Компьютерная безопасность
В. Защищенность информации
Г. Защищенность потребителей информации

30) Непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла АС:

А. Принцип системности
Б. Принцип комплексности
В. Принцип непрерывной защиты
Г. Принцип разумной достаточности
Д. Принцип гибкости системы

Ключ к тесту:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
А	Б	Б,В	А.Б,В	А	Б	В	А	Б	А	А,Б,В	А,Б	В	А	А

16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
А,Б	Б,В	А	В	А	А,Б,В	А,Б	А,Б	Б	Г	Б	Г	Г	А	В

6.2.4. Примерные варианты контрольных работ

Вариант 1.

1. Методы оценки рисков информационной безопасности на предприятии.
2. Генерирование множества альтернатив с применением экспертных методов при разработке СЗИ.
3. Основные этапы принятия управленческих решений в области построения защищенных систем обработки информации.

Вариант 2.

1. Этапы построения защищенных систем обработки информации.
2. “Куб безопасности” в координатах ОСНОВА, НАПРАВЛЕНИЯ, ЭТАПЫ. Обработка трехмерных матриц для оценки эффективности СЗИ.
3. Пример использования метода строчных сумм для составления матрицы альтернативных проектов СЗИ.

Вариант 3.

1. Управление рисками. Модель безопасности с полным перекрытием.
2. Модель элементарной защиты объекта информатизации. Пример расчета прочности защиты.
3. Парное сравнение альтернатив (метод парных сравнений).

Вариант 4.

1. Пример использования сетей Петри для построения сценария действий нарушителя и сигнатур атак.
2. Оценка альтернативных проектов организации СЗИ с использованием критериального метода.
3. Обзор современных программных продуктов для оценки рисков.

Вариант 5.

1. Модель многозвенной защиты объекта информатизации. Пример расчета прочности защиты.
2. Альтернативы и критерии. Требования к набору критериев. Оценка важности критериев.
3. Пример исследования эффективности СЗИ с использованием морфологической матрицы.

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

а) основная литература

1. Анисимов А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс]/ Анисимов А.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 212 с.— Режим доступа: http://www.iprbookshop.ru/15845.— ЭБС «IPRbooks», по паролю

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

3. Галатенко В.А. Основы информационной безопасности [Электронный ресурс]/ Галатенко В.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 266 с.— Режим доступа: http://www.iprbookshop.ru/22424.— ЭБС «IPRbooks», по паролю

б) дополнительная литература

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

2. Аверченков В.И. Аудит информационной безопасности [Электронный ресурс]: учебное пособие для вузов/ Аверченков В.И.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 268 с.— Режим доступа: http://www.iprbookshop.ru/6991.— ЭБС «IPRbooks», по паролю

3. Аграновский А.В. Практическая криптография. Алгоритмы и их программирование [Электронный ресурс]/ Аграновский А.В., Хади Р.А.— Электрон. текстовые данные.— М.: СОЛОН-ПРЕСС, 2009.— 256 с.— Режим доступа: http://www.iprbookshop.ru/8641.— ЭБС «IPRbooks», по паролю

4. Бубнов А. А. Основы информационной безопасности (2-е изд., стер.) учеб. пособие / А. А. Бубнов, В. Н. Пржегорлинский, О. А.Савинкин – М.: Академия, 2016. – 256 с.

5. Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова Е.К.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2012.— 311 с.— Режим доступа: http://www.iprbookshop.ru/10677.— ЭБС «IPRbooks», по паролю

6. Кожуханов Н.М. Правовые основы информационной безопасности [Электронный ресурс]: учебное пособие / Н.М. Кожуханов, Е.С. Недосекова. — Электрон. текстовые данные. — М.: Российская таможенная академия, 2013. — 88 с. — 978-5-9590-0725-6. — Режим доступа:http://www.iprbookshop.ru/69749.html

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации Федеральной службы по техническому и экспортному контролю РФ: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty

2. The logic behind CRAMM’s assessment of measures of risk and determination of appropriate countermeasures. URL: http://www.cramm.com/downloads/techpapers.htm

3. RiskWatch users manual. URL: http://www.riskwatch.com

9. Методические указания для обучающихся по освоению дисциплины

При проведении лекций, практических занятий, самостоятельной работе студентов применяются интерактивные формы проведения занятий с целью погружения студентов в реальную атмосферу профессионального сотрудничества по разрешению проблем, оптимальной выработки навыков и качеств будущего специалиста. Интерактивные формы проведения занятий предполагают обучение в сотрудничестве. Все участники образовательного процесса (преподаватель и студенты) взаимодействуют друг с другом, обмениваются информацией, совместно решают проблемы, моделируют ситуацию.

В учебном процессе используются интерактивные формы занятий:

1. Творческое задание. Выполнение творческих заданий требуют от студента воспроизведение полученной ранее информации в форме, определяемой преподавателем, и требующей творческого подхода.

2. Групповое обсуждение. Групповое обсуждение кого-либо вопроса направлено на достижении лучшего взаимопонимания и способствует лучшему усвоению изучаемого материала.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

В процессе лекционных и практических занятий используется следующее программное обеспечение:

- программы, обеспечивающие доступ в сеть Интернет (например, «Google Chrome»);
- программы, демонстрации видео материалов (например, проигрыватель «Windows Media Player»);
- программы для демонстрации и создания презентаций (например, «Microsoft PowerPoint»);
- программы для реализации алгоритмов шифрования/дешифрования данных, анализа информационных рисков (например, Microsoft Office Excel, Lazarus).

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для преподавания дисциплины требуются специальные материально-технические средства (компьютерный класс). Во время лекционных занятий, которые проводятся в большой аудитории, используется проектор для демонстрации слайдов, схем, таблиц и прочего материала.