Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Кубанский государственный университет»
Экономический факультет

УТВЕРЖДАЮ:
Проректор по учебной работе,
качеству образования – первый
проректор

_____Т.А. Хагуров

«20» ___мая_____ 2020г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

_____ Б1.В.03 Информационная безопасность _____
(код и наименование дисциплины в соответствии с учебным планом)

Направление подготовки ___38.03.02 Менеджмент_____
(код и наименование направления подготовки/специальности)

Направленность (профиль) ___Управление малым бизнесом_
(наименование направленности (профиля) специализации)

Программа подготовки __Прикладная_____
(академическая /прикладная)

Форма обучения _____Очная_____
(очная, очно-заочная, заочная)

Квалификация (степень) выпускника _____Бакалавр_____
(бакалавр, магистр, специалист)

Краснодар 2020

1 Цели и задачи изучения дисциплины (модуля).

1.1 Цель освоения дисциплины.

Формирование знаний основных составляющих информационной безопасности государства, общества и личности; умений и навыков использования организационных, правовых, инженерно-технических и аппаратно-программных методов и средств при построении систем информационной безопасности в области выбранного профиля подготовки.

1.2 Задачи дисциплины.

- обобщить и систематизировать знания по базовым понятиям теории информационной безопасности, знакомство с современными задачами, научной терминологией, моделями и концепциями защиты прав на информатизацию государства, общества и личности и построения систем информационной безопасности;
- приобретение навыков решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;
- приобретение навыков анализа информации о функционировании системы внутреннего документооборота организации, ведения баз данных по различным показателям и формирования информационного обеспечения участников организационных проектов;
- изучение основных положений стратегии информационной войны; основных видов обеспечения систем информационной безопасности, методов оценки уровня защищенности компьютерных систем, методов и средств комплексной защиты объектов информатизации;
- применение организационных, правовых, инженерно-технических и аппаратно-программных методов и средств информационной безопасности в научно-исследовательских и практических разработках в области защиты объектов информатизации.

1.3 Место дисциплины (модуля) в структуре образовательной программы.

Дисциплина «Информационная безопасность» относится к вариативной части Блока 1 "Дисциплины (модули)" учебного плана.

1.4 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы.

Изучение данной учебной дисциплины направлено на формирование у обучающихся (общепрофессиональных и профессиональных компетенций (ОПК- 7, ПК-11)

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
1	ОПК-7	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением	-методы решения стандартных задач профессиональной деятельности на основе информационной и	- решать стандартные задачи профессиональной деятельности на основе информационной и библиографиче	- навыками решения стандартных задач профессиональной деятельности на основе информационной и библиографичес

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
		информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	библиографической культуры; -основы применения безопасных информационно-коммуникационных технологий; -основные требования информационной безопасности;	ской культуры; - применять безопасные информационно-коммуникационные технологии; - реализовывать на практике требования информационной безопасности;	кой культуры; - навыками применения безопасных информационно-коммуникационных технологий; - навыками реализации требований информационной безопасности;
2	ПК-11	владением навыками анализа информации о функционировании системы внутреннего документооборота организации, ведения баз данных по различным показателям и формирования информационного обеспечения участников организационных проектов	- основы анализа информации о функционировании системы внутреннего документооборота организации; - основы безопасного ведения баз данных по различным показателям и формирования информационного обеспечения участников организационных проектов;	- анализировать информацию о функционировании системы внутреннего документооборота организации; - безопасно вести базы данных по различным показателям и формировать информационное обеспечение участников организационных проектов;	- навыками анализа информации о функционировании системы внутреннего документооборота организации; - навыками безопасного ведения базы данных по различным показателям и формирования информационного обеспечения участников организационных проектов.

2. Структура и содержание дисциплины.

2.1 Распределение трудоёмкости дисциплины по видам работ.

Общая трудоёмкость дисциплины составляет 2 зач.ед. (72 часов), их распределение по видам работ представлено в таблице.

Вид учебной работы	Всего часов	Семестры (часы)			
		4			
Контактная работа, в том числе:					
Аудиторные занятия (всего):	**36**	**36**			
Занятия лекционного типа	18	18	-	-	-
Лабораторные занятия	18	18	-	-	-
Занятия семинарского типа (семинары,	-	-	-	-	-

практические занятия)						
		-	-	-	-	-
Иная контактная работа:						
Контроль самостоятельной работы (КСР)		4	4			
Промежуточная аттестация (ИКР)		0,2	0,2			
Самостоятельная работа, в том числе:						
Проработка учебного (теоретического) материала		12	12	-	-	-
Выполнение индивидуальных заданий (Подготовка деловой игры «Защита информации предприятия»)		8	8	-	-	-
Подготовка к текущему контролю		11,8	11,8	-	-	-
Контроль:						
Подготовка к экзамену		-	-	-	-	-
Общая трудоемкость	**час.**	**72**	**72**	**-**	**-**	**-**
	в том числе контактная работа	**40,2**	**40,2**			
	зач. ед	**2**	**2**			

2.2 Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы дисциплины, изучаемые в 4 семестре

№	Наименование тем	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1.	Раздел 1. Введение в дисциплину	15,8	4	-	2	7,8
2.	Раздел 2. Основы государственной политики РФ в области информационной безопасности	14	4	-	2	8
3.	Раздел 3. Информационная война.	14	4	-	2	8
4.	Раздел 4. Основы обеспечения информационной безопасности компьютерных систем (КС)	26	6	-	12	8
	Итого по дисциплине:		18	-	18	31,8

Примечание: Л – лекции, ПЗ – практические занятия / семинары,ЛР – лабораторные занятия, СРС – самостоятельная работа студента

2.3 Содержание тем дисциплины:

2.3.1 Занятия лекционного типа.

№	Наименование темы	Содержание темы	Форма текущего контроля
1	2	3	4
1.	Раздел 1. Введение в дисциплину	Раздел 1. Введение в дисциплину 1.1 Понятие национальной безопасности РФ 1.2 Виды безопасности 1.3 Информационная безопасность в системе национальной безопасности РФ 1.4 Роль информационной безопасности в обеспечении национальной безопасности государства	Л,Д

2.	Раздел 2. Основы государственной политики РФ в области информационной безопасности	Раздел 2. Основы государственной политики РФ в области информационной безопасности 2.1 Национальные интересы РФ в информационной сфере и их обеспечение 2.2 Виды угроз информационной безопасности РФ 2.3 Источники угроз информационной безопасности 2.4 Основные направления обеспечения информационной безопасности государства	Л,Д
3.	Раздел 3. Информационная война.	Раздел 3. Информационная война. 3.1 Методы и средства ее ведения 3.2 Информационная безопасность и информационное противоборство 3.3 Информационное оружие, его классификация и возможности 3.4 Обеспечение информационной безопасности объектов информационной сферы государства в условиях информационной войны	Л,Д
4.	Раздел 4. Основы обеспечения информационной безопасности компьютерных систем (КС)	Раздел 4. Основы обеспечения информационной безопасности компьютерных систем (КС) 4.1 Организационно-правовые основы информационной безопасности КС 4.2 Организационно-технические основы ИБ КС 4.3 Аппаратно-программные средства обеспечения ИБ КС 4.4 Основы комплексного обеспечения ИБ КС	Л,Д

2.3.2 Занятия семинарского типа.

не предусмотрены учебным планом

2.3.3 Лабораторные занятия

№	Наименование темы	Содержание темы	Форма текущего контроля
1	2	3	4
1.	Раздел 1. Введение в дисциплину	Изучение методов защиты от разрушающих программных воздействий при помощи программных комплексов антивирусной защиты	ЛР
2.	Раздел 2. Основы государственной политики РФ в области информационной безопасности	Изучение методов защиты при помощи программно-аппаратного комплекса Secret Net	ЛР
3.	Раздел 3. Информационная война.	" Шифрование и обмен шифрованной информацией с использованием системы «PGP»	ЛР

4.	Раздел 4. Основы обеспечения информационной безопасности компьютерных систем (КС)	Применение специализированных средств организации VPN на примере «OpenVpn»	ЛР

Защита лабораторной работы (ЛР), выполнение курсового проекта (КП), курсовой работы (КР), расчетно-графического задания (РГЗ), написание реферата (Р), эссе (Э), коллоквиум (К), тестирование (Т), опрос (О), лекция (Л), дискуссия (Д) и т.д.

Содержание лабораторных занятий

Занятие 1 Изучение методов защиты от разрушающих программных воздействий при помощи программных комплексов антивирусной защиты

Занятие 2 Изучение методов защиты при помощи программно-аппаратного комплекса Secret Net

Занятие 3" Шифрование и обмен шифрованной информацией с использованием системы «PGP»

Занятие 4 Применение специализированных средств организации VPN на примере «OpenVpn» Способы защиты программ от дизассемблирования

2.3.4 Примерная тематика курсовых работ (проектов)

Курсовые работы (проекты) не предусмотрены учебным планом.

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1.	Проработка учебного (теоретического) материала по теме: Введение в дисциплину	Методические указания по выполнению самостоятельной работы обучающихся. Утверждены на заседании Совета экономического факультета ФГБОУ ВО «КубГУ». Протокол № 8 от 29 июня 2017 г. Режим доступа: https://www.kubsu.ru/ru/econ/metodicheskie
2.	Проработка учебного (теоретического) материала по теме: Основы государственной политики РФ в области информационной безопасности	Методические указания по выполнению самостоятельной работы обучающихся. Утверждены на заседании Совета экономического факультета ФГБОУ ВО «КубГУ». Протокол № 8 от 29 июня 2017 г. Режим доступа: https://www.kubsu.ru/ru/econ/metodicheskie
3.	Проработка учебного (теоретического) материала по теме: Информационная	Методические указания по выполнению самостоятельной работы обучающихся. Утверждены на заседании Совета экономического факультета ФГБОУ ВО «КубГУ».

	война.	Протокол № 8 от 29 июня 2017 г. Режим доступа: https://www.kubsu.ru/ru/econ/metodicheskie
4.	Проработка учебного (теоретического) материала по теме: Основы обеспечения информационной безопасности компьютерных систем (КС)	Методические указания по выполнению самостоятельной работы обучающихся. Утверждены на заседании Совета экономического факультета ФГБОУ ВО «КубГУ». Протокол № 8 от 29 июня 2017 г. Режим доступа: https://www.kubsu.ru/ru/econ/metodicheskie
5.	Выполнение индивидуальных заданий (Подготовка деловой игры «Защита информации предприятия»)	Методические указания по выполнению самостоятельной работы обучающихся. Утверждены на заседании Совета экономического факультета ФГБОУ ВО «КубГУ». Протокол № 8 от 29 июня 2017 г. Режим доступа: https://www.kubsu.ru/ru/econ/metodicheskie

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

–в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа,

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

3. Образовательные технологии.

В процессе изучения дисциплины используются современные формы проведения занятий. Демонстрационные материалы представлены в форме интерактивных презентаций по темам лекционного курса. Комплекты схем к темам «Введение в дисциплину », «Основы государственной политики РФ в области информационной безопасности», «Информационная война», «Основы обеспечения информационной безопасности компьютерных систем (КС)»,.

Раздаточные материалы используются в процессе лекционных и практических занятий для наглядной демонстрации тех или иных аспектов прикладного исследования.

Примерная модель служб предприятия для подготовки деловой игры.

Проект деловой игры «Защита информации предприятия»

Лекция-диалог. Содержание подается через серию вопросов, на которые слушатель должен отвечать непосредственно в ходе лекции. К этому типу примыкает лекция с применением техники обратной связи, а также программированная лекция-консультация;

Проблемная лекция начинается с вопросов, с постановки проблемы, которую в ходе изложения материала необходимо решить. Проблемные вопросы отличаются от не проблемных тем, что скрытая в них проблема требует не однотипного решения, то есть, готовой схемы решения в прошлом опыте нет.

Лекции-диалоги и проблемные лекции позволяют включать интерактивные элементы в процесс преподавания, способствуют приобретению не только знаний по теме лекции, но и навыков исследовательской и аналитической деятельности.

Лекции в форме презентации с использованием мультимедийной аппаратуры обеспечивают более высокий уровень понимания сложных структур, схем взаимосвязей отдельных элементов.

Лабораторные занятия предполагают организацию выполнения задания по поиску или решению конкретной задачи с использованием ПЭВМ по отдельным вопросам, что способствует формированию более глубоких знаний по теме, а также развитию навыков поиска, анализа необходимой информации, навыков публичной защиты своей позиции.

Интерактивные и информационно-коммуникативные образовательные технологии, используемые в аудиторных занятиях, в сочетании с внеаудиторной работой создают дополнительные условия формирования и развития требуемых компетенций обучающихся, поскольку позволяют обеспечить активное взаимодействие всех участников. Эти методы способствуют личностно-ориентированному подходу.

Для инвалидов и лиц с ограниченными возможностями здоровья устанавливается особый порядок освоения указанной дисциплины. В образовательном процессе используются социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе. Вышеозначенные образовательные технологии дают наиболее эффективные результаты освоения дисциплины с позиций актуализации содержания темы занятия, выработки продуктивного мышления, терминологической грамотности и компетентности обучаемого в аспекте социально-направленной позиции будущего специалиста, и мотивации к инициативному и творческому освоению учебного материала. Рекомендации по использованию интерактивных и информационных образовательных технологий были осуществлены согласно методических указаниям к подобного рода работам. Режим доступа: https://www.kubsu.ru/ru/econ/metodicheskie-ukazaniya.

Индивидуальные консультации обучающихся проводятся еженедельно в форме диалога. Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации.

4.1Фонд оценочных средств для проведения текущего контроля.

Раздел 1. Введение в дисциплину

Понятие национальной безопасности РФ

Виды безопасности

Информационная безопасность в системе национальной безопасности РФ

Роль информационной безопасности в обеспечении национальной безопасности государства

Раздел 2. Основы государственной политики РФ в области информационной безопасности

2.1 Национальные интересы РФ в информационной сфере и их обеспечение

2.2 Виды угроз информационной безопасности РФ

2.3 Источники угроз информационной безопасности

2.4 Основные направления обеспечения информационной безопасности государства

Раздел 3. Информационная война.

3.1 Методы и средства ее ведения

3.2 Информационная безопасность и информационное противоборство

3.3 Информационное оружие, его классификация и возможности

3.4 Обеспечение информационной безопасности объектов информационной сферы государства в условиях информационной войны

Раздел 4. Основы обеспечения информационной безопасности компьютерных систем (КС)

4.1 Организационно-правовые основы информационной безопасности КС

4.2 Организационно-технические основы ИБ КС

4.3 Аппаратно-программные средства обеспечения ИБ КС

4.4 Основы комплексного обеспечения ИБ КС

4.2 Фонд оценочных средств для проведения промежуточной аттестации.

Вопросы к зачету

1. Информационная безопасность человека и общества и государства.
2. Уровни защиты информационных ресурсов. Признаки, свидетельствующие о наличии уязвимых мест в информационной безопасности.
3. Компьютерные преступления. Основные технологии, использующиеся при совершении компьютерных преступлений.
4. Объекты защиты информации. Защита информации ограниченного доступа: государственная тайна, коммерческая тайна.
5. Основные каналы утечки информации. Защита от утечки информации по техническим каналам.
6. Методы и средства защиты информации.
7. Содержание способов и средств обеспечения безопасности информации.
8. Реализация методов и средств защиты информации.
9. Средства опознания и разграничения доступа к информации.
10. Криптография. Симметричные криптосистемы.
11. Криптография. Асимметричные криптосистемы.
12. Обзор и классификация методов шифрования информации.
13. Электронно-цифровая подпись.
14. Основные алгоритмы шифрования данных: ГОСТ.
15. Правовые средства защиты информации. Защита программных продуктов. Авторское право.
16. Защита данных в автономном компьютере.
17. Защита данных в вычислительных сетях.
18. Разработка сетевых аспектов политики безопасности.
19. Защита данных в вычислительных сетях. Межсетевые экраны. Сканеры.
20. Показатели оценки достоверности (безошибочности) передачи данных в сетях.
21. Методы взлома компьютерных систем: атаки на уровне операционных систем, атаки на уровне программного обеспечения, атаки на уровне систем управления базами данных.
22. Парольная защита операционных систем.
23. Парольные взломщики.
24. Понятие угрозы. Анализ угроз информационной безопасности. Виды «нарушителей».
25. Структуризация методов обеспечения информационной безопасности.
26. Основные методы реализации угроз информационной безопасности.

27. Основные принципы обеспечения информационной безопасности в автоматизированной системе.
28. Причины, виды и каналы утечки информации.
29. Методы построения защищенных автоматизированных систем.
30. Политика безопасности. Основные типы политики безопасности.
31. Политика безопасности. Модели безопасности.
32. Стандарты информационной безопасности.
33. Правовое обеспечение защиты информации. Нормативные документы.
34. Разрушающие программные воздействия: вирусы и закладки.
35. Антивирусные средства.
36. Психологические аспекты информационной безопасности организации.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля).

5.1 Основная литература:

1. Нестеров, С.А. Информационная безопасность : учебник и практикум / С. А. Нестеров. — М. : Издательство Юрайт, 2018. — 321 с. — Режим доступа : www.biblio-online.ru/book/836C32FD-678E-4B11-8BFC-F16354A8AFC7

2. Попов И.И. Информационная безопасность : учеб. пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — М. : ФОРУМ : ИНФРА-М, 2018. — 432 с. — Режим доступа: http://znanium.com/bookread2.php?book=915902

3. Баранова Е.К. Информационная безопасность и защита информации: Учебное пособие / Баранова Е.К., Бабаш А.В., - 4-е изд., перераб. и доп. - М.:ИЦ РИОР, НИЦ ИНФРА-М, 2018. - 336 с. — Режим доступа: http://znanium.com/bookread2.php?book=957144

Для освоения дисциплины инвалидами и лицами с ограниченными возможностями здоровья имеются издания в электронном виде в электронно-библиотечных системах «Университетская библиотека онлайн».

Многоуровневая система навигации ЭБС позволяет оперативно осуществлять поиск нужного раздела. Личный кабинет индивидуализирован, то есть каждый пользователь имеет личное пространство с возможностью быстрого доступа к основным смысловым узлам.

При чтении масштаб страницы можно увеличить, можно использовать полноэкранный режим отображения книги или включить озвучивание текста непосредственно с сайта при помощи программ экранного доступа, например, Jaws, «Balabolka».

Скачиваемые фрагменты в формате pdf, содержащие подтекстовый слой, достаточно высокого качества и могут использоваться тифлопрограммами для голосового озвучивания текстов, быть загружены в тифлоплееры (устройств для прослушивания книг), а также скопированы на любое устройство для комфортного чтения.

В ЭБС представлена медиатека, которая включает в себя различные тематические аудио книги различных издательств. Контент ЭБС активно пополняется книгами и учебниками в международном стандартизированном формате Daisy для незрячих, основу которого составляют гибкая навигация и защищенность контента.

5.2 Дополнительная литература:

1. Гришина Н.В. Информационная безопасность предприятия: Учебное пособие / Гришина Н.В., - 2-е изд., доп - М.:Форум, НИЦ ИНФРА-М, 2016. - 240 с. — Режим доступа: http://znanium.com/bookread2.php?book=544554

2. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей : учеб. пособие / В.Ф. Шаньгин. — М. : ИД «ФОРУМ» : ИНФРА-М, 2017. — 416 с. — Режим доступа: http://znanium.com/bookread2.php?book=775200

3. Мецатунян М.В. Основные положения информационной безопасности : учеб. пособие / В.Я. Ищейнов, М.В. Мецатунян. — М. : ФОРУМ : ИНФРА-М, 2018. — 208 с. — Режим доступа: http://znanium.com/bookread2.php?book=927190

4. Нестеров, С.А. Основы информационной безопасности : учебное пособие / С.А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. - Санкт-Петербург : Издательство Политехнического университета, 2014. - 322 с. — Режим доступа: http://biblioclub.ru/index.php?page=book&id=363040

5. Краткий энциклопедический словарь по информационной безопасности : словарь / сост. В.Г. Дождиков, М.И. Салтан. - Москва : Энергия, 2010. - 240 с. — Режим доступа: http://biblioclub.ru/index.php?page=book&id=58393

5.3. Периодические издания:

Журналы:

- КомпьютерПресс;
- Программные продукты и системы;
- Информация и безопасность;
- Информационная безопасность.

6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

http://mk-company.ucoz.ru/index/informacionnaja_bezopasnost/0-9

http://www.securrity.ru/articles/196-ederal_law_of_the_information_security.html

http://www.scrf.gov.ru/documents/5.html

https://www.securitycode.ru/products/demo-versions/

https://addons.mozilla.org/ru/thunderbird/extensions/
http://free-vpn.ru/openvpn.html

7. Методические указания для обучающихся по освоению дисциплины (модуля).

Самостоятельная работа предусматривает самостоятельное освоение отдельных вопросов и проблем в рамках учебной дисциплины. В процессе самостоятельной работы слушатели знакомятся с содержанием научных статей и монографий, составляют тезисы, осуществляют подготовку к семинарским занятиям, опираясь на список литературы и дополнительные списки к темам самостоятельной подготовки.

Вопросы, выносимые на самостоятельное изучение.

Доктрина Российской Федерации.

Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.

Общие вопросы организации противодействия технической разведке; основные организационные и технические мероприятия, используемые для противодействия технической разведке.

Методы и средства защиты режимных объектов от утечки конфиденциальной информации по техническим каналам; физические основы образования побочных электромагнитных излучений от технических средств; каналы утечки информации

Основные этапы жизненного цикла вирусов. Объекты внедрения, режимы функционирования и специальные функции вирусов. Схемы заражения файлов. Схемы заражения загрузчиков. Способы маскировки, используемые вирусами. Классификация компьютерных вирусов. Общая организация защиты от компьютерных вирусов.

Способы защиты от несанкционированного использования остаточной информации. Использование специализированных программ по уничтожению остаточных данных. Специальные режимы и особенности шифрования данных в режиме реального времени с возможность мгновенного уничтожения данных.

Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование

Базовые этапы построения системы комплексной защиты вычислительных систем. Анализ моделей нарушителя. Угрозы информационно-программному обеспечению вычислительных систем и их классификация.

Использование FoxitReader 6.1.3.321 PGP Desktop 9.5 beta demo, Secret Net demo, Mozilla Thunderbird с дополнением Enigmail (free), OpenVPN (free).

Методы и средства ограничения доступа к компонентам ЭВМ, надежность средств защиты компонент; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором, способствующими индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю).

8.1 Перечень информационных технологий.

Скоростной доступ к сети Интернет (10 Мбит/с), что дает возможность студентам и сотрудникам свободно пользоваться информационными сетями различного уровня.

Локальные сети (две), 4 компьютерных класса, включающих 67 рабочих мест IBM PC совместимых компьютеров, оснащенных современным программных обеспечением и выходом в информационно-коммуникационную образовательную среду, в т.ч. Moodle.

8.2 Перечень необходимого программного обеспечения.

Microsoft Windows 10 , GoogleChrome 63.0.3239.84, MicrosoftOfficeProfessionalPlus 2013 15.0.4569.1506.

8.3Перечень информационных справочных систем:

1. Электронная библиотечная система eLIBRARY.RU (http://www.elibrary.ru)/

2.Электронная библиотечная система «Университетская библиотека онлайн» (http://www.biblioclub.ru)

3. Электронная библиотечная система«Юрайт» (https://biblio-online.ru)

4. Электронная библиотечная система «ZNANIUM.COM» (http://znanium.com)

9. Материально-техническая база, необходимая для осуществления образовательногопроцесса по дисциплине (модулю)

№	Вид работ	Материально-техническое обеспечение дисциплины (модуля) и оснащенность
1.	Лекционные занятия	Лекционная аудитория 520А, 207Н, 208Н, 209Н, 212Н, 214Н, 201А, 205А, 4033Л, 4038Л, 4039Л, 5040Л, 5041Л, 5042Л, 5045Л, 5046Л, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) и соответствующим программным обеспечением (ПО) MicrosoftOffice.
2.	Семинарские занятия не предусмотрены учебным планом	Специальное помещение 2026Л, 2027Л, 4034Л, 4035Л, 4036Л, 5043Л, 201Н, 202Н, 203Н, А203Н, оснащенное презентационной техникой (проектор, экран, ноутбук) и прикладным программным обеспечением (MicrosoftOffice), а также аудитории А208Н, 202А, 210Н, 216Н, 513А, 514А, 515А, 516А.
3.	Лабораторные занятия	Лаборатория 201Н, 202Н, 203Н, А203Н, 205А, укомплектованная специализированной мебелью и техническими средствами обучения. Рабочие места, подключены к локальной сети факультета, имеют доступ к глобальной сети Интернет.
4.	Групповые (индивидуальные) консультации	Аудитория 224
5.	Текущий контроль, промежуточная аттестация	Аудитория 520А, 207Н, 208Н, 209Н,212Н, 214Н, 201А,205А,А208Н, 202А, 210Н, 216Н, 513А, 514А, 515А, 516А,2026Л, 2027Л, 4033Л, 4034Л, 4035Л, 4036Л, 4038Л, 4039Л, 5040Л, 5041Л, 5042Л, 5043Л, 5045Л, 5046Л, 201Н, 202Н, 203Н, А203Н укомплектованные презентационной техникой (проектор, экран, ноутбук) и прикладным программным обеспечением (MicrosoftOffice).
6.	Самостоятельная работа	Кабинет для самостоятельной работы, оснащенный компьютерной техникой с возможностью подключения к

		сети «Интернет»,программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета.

10. Перечень необходимых информационных справочных систем и современных профессиональных баз данных

Обучающимся обеспечен доступ к современным профессиональным базам данных, профессиональным справочным и поисковым системам:

1. **Консультант Плюс - справочная правовая система http://www.consultant.ru;**
2. **База данных международных индексов научного цитирования Web of Science (WoS) http://webofscience.com/;**
3. **База данных рефератов и цитирования Scopus http://www.scopus.com/;**
4. **Базы данных компании «Ист Вью» http://dlib.eastview.com;**
5. **База открытых данных Росстата http://www.gks.ru/opendata/dataset;**