Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Кубанский государственный университет»
(ФГБОУ ВО «КубГУ»)

Физико-технический факультет

УТВЕРЖДАЮ:
Проректор по учебной работе,
качеству образования – первый
проректор
_____ Хагуров Т.А.
подпись
«_27_» _____ 2018 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.12.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Направление подготовки 09.03.02 Информационные системы и технологии

Направленность (профиль) Информационные системы и технологии

Программа подготовки академический бакалавриат

Форма обучения очная

Квалификация (степень) выпускника бакалавр

Краснодар 2018

Рабочая программа дисциплины Б1.В.ДВ.12.01 Информационная безопасность и защита информации составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 09.03.02 «Информационные системы и технологии».

Программу составил(и):
Н.Н. Куликова, преподаватель кафедры теоретической физики и компьютерных технологий,
кандидат биологических наук


подпись

Рабочая программа дисциплины Б1.В.ДВ.12.01 Информационная безопасность и защита информации утверждена на заседании кафедры теоретической физики и компьютерных технологий
протокол № 9 «29» марта 2018 г.
Заведующий кафедрой (разработчика) Исаев В.А.


подпись

Рабочая программа обсуждена на заседании кафедры теоретической физики и компьютерных технологий
протокол № 9 «29» марта 2018 г.
Заведующий кафедрой (выпускающей) Исаев В.А.


подпись

Утверждена на заседании учебно-методической комиссии физико-технического факультета
протокол № 10 «12» апреля 2018г.
Председатель УМК факультета Богатов Н.М.


подпись

Рецензенты:

Н.М. Богатов, зав. кафедрой
физики и информационных
систем КубГУ, д. ф.-м. н.


подпись

Л.Р. Григорьян, ген. директор
ООО НПФ «Мезон», к. ф.-м. н.


подпись

1 Цели и задачи изучения дисциплины.

1.1 Цель дисциплины.

Целью дисциплины Б1.В.ДВ.12.01 «Информационная безопасность и защита информации» является освоение базовых знаний в области защиты информации, анализа стойкости алгоритмов шифрования, овладение компетенциями по квалифицированному применению на практике профессиональной терминологии, по классификации защищаемой информации средств и систем её защиты, проведению целенаправленного поиска в различных источниках информации по защите информации, в том числе в глобальных компьютерных системах.

1.2 Задачи дисциплины.

Задачи изучения дисциплины являются изучение:

- организационно-правовых основ защиты информации;
- методы и средства защиты информации;
- организационно-правовые и инженерно-технические особенности защиты конфиденциальной информации и персональных данных;
- основ применения криптографических методов, принципов синтеза и анализа криптосистем, математических методов, используемых для оценки стойкости криптосистем.

1.3 Место дисциплины (модуля) в структуре образовательной программы.

Дисциплина «Информационная безопасность и защита информации» относится к вариативной части Блока 1 «Дисциплины (модули)» учебного плана профиля «Информационные системы и технологии» и ориентирована при подготовке бакалавров на изучение методов и средств защиты информации, приобретение умений и навыков в защите компьютерной информации. Дисциплина «Информационная безопасность и защита информации» находится в логической и содержательно-методологической взаимосвязи с другими частями ООП и базируется на знаниях, полученных при изучении дисциплин «Информатика», «Информационные технологии», «Технологии программирования С/С++», «Теория информационных процессов и систем». Знания, навыки и умения, приобретенные в результате изучения дисциплины, будут востребованы при выполнении курсовых и дипломных работ, связанных с работой прикладного программного обеспечения, а также информационных систем, ориентированных многопользовательский режим работы, или же на работу в сети Интернет.

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 общепрофессиональной и профессиональных компетенций (ОПК-4, ПК-11, ПК-13).

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
1.	ОПК- 4	пониманием сущности и значения информации в развитии современного информационного общества, соблюдение основных требований к информационной безопасности, в том числе защите	основные понятия методов и моделей информационной безопасности	осознавать опасности и угрозы, возникающие в процессе развития информационных технологий	навыками информационной безопасности

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
		государственной тайны			
2.	ПК-11	способностью к проектированию базовых и прикладных информационных технологий	основные понятия и направления в защите компьютерной информации, принципы защиты информации, принципы классификации и примеры угроз безопасности компьютерным системам, современные подходы к защите продуктов и систем информационных технологий, реализованные в действующих отечественных и международных стандартах ИТ-безопасности	проводить анализ защищенности компьютера и сетевой среды, устанавливать и настраивать программное обеспечение для защиты от вредоносного ПО; конструировать криптостойкие алгоритмы и протоколы, создавать программы, реализующие алгоритмы и протоколы защищенной передачи данных	методами аудита безопасности информационных систем, методами системного анализа, навыками использования типовых криптографических алгоритмов
3.	ПК-13	способностью разрабатывать средства автоматизированного проектирования информационных технологий	основные инструменты обеспечения многоуровневой безопасности в информационных системах, основные направления криптографии и теории кодирования, принципы построения и основные виды симметричных и асимметрич-	обеспечивать защиту информации с использованием программно-аппаратных средств, конфигурировать встроенные средства безопасности в ОС	знаниями о требованиях к шифрам и основных характеристиках шифров

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
			ных криптографических алгоритмов, математические модели шифров		

2. Структура и содержание дисциплины.

2.1 Распределение трудоёмкости дисциплины по видам работ.

Общая трудоёмкость дисциплины составляет 4 зач.ед. (144 часа), их распределение по видам работ представлено

(для студентов ОФО).

Вид учебной работы		Всего часов	Семестры (часы)			
			7			
Контактная работа, в том числе:						
Аудиторные занятия (всего):		**64**	**64**	-	-	-
Занятия лекционного типа		32	32	-	-	-
Лабораторные занятия		32	32	-	-	-
Занятия семинарского типа (семинары, практические занятия)		-	-	-	-	-
Иная контактная работа:						
Контроль самостоятельной работы (КСР)		4	4	-	-	-
Промежуточная аттестация (ИКР)		0,3	0,3	-	-	-
Самостоятельная работа, в том числе:		**49**	**49**	-	-	-
Проработка учебного (теоретического) материала		20	20	-	-	-
Реферат		9	9			
Подготовка к текущему контролю		20	20	-	-	-
Контроль:						
Подготовка к экзамену		26,7	26,7	-	-	-
Общая трудоемкость	**час.**	**144**	**144**	-	-	-
	в том числе контактная работа	**68,3**	**68,3**	-	-	-
	зач. ед	**4**	**4**	-	-	-

2.2 Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы дисциплины, изучаемые в 7 семестре *(очная форма)*

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1.	Концептуальные основы информационной безопасности	18	6	-	2	10
2.	Организационно-правовые аспекты защиты информации	19	4	-	2	13
3.	Математические методы и модели в задачах защиты информации	41	8	-	20	13
4.	Многоуровневая защита информации в компьютерных системах и сетях	35	14	-	8	13
	Итого по дисциплине:	113	32	-	32	49

2.3 Содержание разделов дисциплины:

2.3.1 Занятия лекционного типа.

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
Концептуальные основы информационной безопасности			
1.	Понятие, сущность, цели и концептуальные основы защиты информации	Общий контекст защиты информации. Понятие «защита информации». Сущность и содержание защиты информации. Цели и задачи защиты информации. Концептуальная модель защиты информации.	ЛР
2.	Угрозы информационной безопасности	Анализ угроз информационной безопасности. Классификация потенциальных атакующих сторон. Спецификация атак на объект защиты. Методы компенсации угроз информационной безопасности.	ЛР
3.	Каналы несанкционированного получения информации	Классификация методов и средств НСД. Человеческий фактор при НСД. Каналы утечки информации и способы НСД к компьютеру. Акустические каналы. Прослушивание телефонных переговоров. Скремблирование	ЛР,Р
Организационно-правовые аспекты защиты информации			
4.	Законодательство в области информационной безо-	Организационные методы защиты. Законодательные и правовые осно-	ЛР

	пасности	вы защиты информации. принципы разработки политики безопасности, основные положения "Закона о персональных данных". Обзор международных стандартов в области информационной безопасности	
5.	Создание политики безопасности ИС	Концепция, стандарты, процедуры, модели, методы. Взаимодействие с различными типами пользователей.	ЛР
Математические методы и модели в задачах защиты информации			
6.	Основы криптоанализа	Цели и задачи криптоанализа. Криптографическая устойчивость информационных систем. Градиентная статистическая атака.	ЛР
7.	Криптография с открытым ключом	Модель передачи сообщения в криптосистеме с открытым ключом. Основы теории чисел. Понятие односторонней функции, примеры односторонней функции	Р
8.	Криптографические протоколы	Понятие криптографического протокола. Электронные деньги. Задача о взаимной верификации.	ЛР, Р
9.	Шифры с секретным ключом	Понятие блокового шифра. Режимы функционирования блоковых шифров. Понятие идеального шифра. Потоковые шифры. Криптографические хэш-функции.	ЛР
Многоуровневая защита информации в компьютерных системах и сетях			
10.	Идентификация и аутентификация	Статическая аутентификация. Устойчивая аутентификация. Постоянная аутентификация. Токены. Электронные подписи.	ЛР
11.	Ключи, защита программ.	Защита программ от несанкционированного копирования. Ключи. Проблемы защиты и взлома программ. Системы защиты персональных данных.	ЛР
12.	Межсетевые экраны, как средство от НСД из общедоступных сетей.	История. Общие понятия. Основные компоненты МЭ. Типовые схемы защиты с использованием МЭ.	ЛР
13.	Программы с потенциально опасными последствиями	Вирус. Люк. Троянский конь. Логическая бомба. Программные закладки. Меры защиты.	ЛР,Р
14.	Разработка приложений	Защита интеллектуальной собственности программного обеспечения. Проектирование механизмов безопасности. Контроль жизненного цикла программного обеспечения.	ЛР

2.3.2 Занятия семинарского типа.

Занятия семинарского типа не предусмотрены.

2.3.3 Лабораторные занятия.

№	Наименование раздела	Наименование лабораторных работ	Форма текущего контроля
1	2	3	4
1.	Концептуальные основы информационной безопасности	1. Концептуальные основы информационной безопасности предприятия 2. Анализ рисков информационной безопасности. Построение концепции информационной безопасности предприятия	ЛР
2.	Организационно-правовые аспекты защиты информации		ЛР
3.	Математические методы и модели в задачах защиты информации	3. Простейшие криптографические алгоритмы. 4. Программная реализация криптографических алгоритмов 5. Механизмы контроля целостности данных 6. Алгоритмы поведения вирусных и других вредоносных программ 7. Алгоритмы предупреждения и обнаружения вирусных угроз 8. Пакеты антивирусных программ	ЛР
4.	Многоуровневая защита информации в компьютерных системах и сетях	9. Выбор программно-аппаратного обеспечения для проектирования защищенной сети передачи данных	ЛР

2.3.4 Примерная тематика курсовых работ (проектов).
Курсовые работы не предусмотрены.

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	Методические указания по организации аудиторной и самостоятельной работ, утвержденные кафедрой теоретической физики и компьютерных технологий, протокол № 9 от «14» марта 2017г
2	Реферат	1.Методические рекомендации по написанию реферата, утвержденные кафедрой теоретической физики и компьютерных технологий, протокол № 9 от «14» марта 2017г. 2.Бушенева Ю.И. Как правильно написать реферат, курсовую и дипломную работы: Учебное пособие для бакалавров [Электронный ресурс]: учеб. пособие – Электрон. дан. – М.:

		Дашков и К, 2016. – 140 с. Режим доступа: https://e.lanbook.com/book/93331
3	Подготовка к текущему контролю	Методические рекомендации для подготовки к практическим, семинарским и лабораторным занятиям, утвержденные кафедрой теоретической физики и компьютерных технологий, протокол № 9 от «14» марта 2017г.

3. Образовательные технологии.

Получение углубленных знаний по изучаемой дисциплине достигается за счет дополнительных часов к аудиторной работе – самостоятельной работы студентов. Выделяемые часы целесообразно использовать для знакомства с дополнительной научной литературой по проблематике дисциплины, анализа научных концепций и практических рекомендаций лидеров бизнеса – ведущих российских и зарубежных компаний, организаций.

В современных условиях развитие продуктивных технологий в сфере образования становится неотъемлемой частью процесса модернизации. Заканчиваются возможности экстенсивного пути развития образования, при котором повышение образованности и профессиональности связывалось с увеличением объема знаний, и начинается переход к интенсивному пути развития образования. Он требует становления принципиально новых образовательных подходов в противовес широко распространенным сегодня репродуктивным технологиям, основанным на простом воспроизводстве информации. Новые технологии должны базироваться на продуктивности, креативности, мобильности и опираться на научное мышление, формирование которого у обучающихся становится основной задачей образовательного процесса.

1. Дискуссия.
2. Анализ ситуаций профессиональной деятельности
3. Метод проектов.
4. Метод малых групп
5. Интерактивная лекция (беседа, лекция – дискуссия, лекция с разбором конкретных ситуаций)

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью ООП, особенностью контингента обучающихся и содержанием конкретных дисциплин, и в целом в учебном процессе должен составлять не менее 10 процентов от общего объема аудиторных занятий.

Так как общий объем аудиторных занятий по дисциплине «Информационная безопасность и защита данных» на *очной форме обучения* составляет 144 часов, то занятия, проводимые в интерактивных формах, должны составлять не менее 14 часов. Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

Используемые интерактивные образовательные технологии по семестрам и видам занятий на *очной форме обучения* представлены в таблице.

Семестр	Вид занятий (Л, ЛР)	Используемые интерактивные технологии	Количество часов
7	Л	Интерактивная лекция Анализ ситуаций профессиональной деятельности	6
	ЛР	Дискуссия Метод проектов Метод малых групп	8
Итого:			14

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

4.1 Фонд оценочных средств для проведения промежуточной аттестации.

Вопросы к экзамену:

1. Государственная политика в сфере обеспечения информационной безопасности.
2. Понятие информационной безопасности. Принципы обеспечения информационной безопасности.
3. Основные информационные права и свободы на доступ к информации и их ограничения.
4. Основные конституционные гарантии права на доступ к информации.
5. Защита права на доступ к информации. Ответственность за нарушение прав и свобод.
6. Право на неприкосновенность частной жизни. Ограничения прав субъектов на неприкосновенность частной жизни.
7. Конституционные гарантии права на неприкосновенность частной жизни.
8. Способы защита неприкосновенности частной жизни.
9. Персональные данные как особый институт охраны прав на неприкосновенность частной жизни.
10. Информация с ограниченным доступом: понятие критерии (условия) охраноспособности.
11. Правовое регулирование деятельности средств массовой информации в информационной сфере.
12. Виды информации с ограниченным доступом. Краткая характеристика каждого вида.
13. Государственная тайна. Перечень сведений составляющих государственную тайну. Грифы секретности.
14. Органы защиты государственной тайны.
15. Лицензирование деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны.
16. Понятие коммерческой тайны. Критерии (условия) охраноспособности информации, отнесенной к коммерческой тайне.
17. Способы защиты права на коммерческую тайну.
18. Ответственность, установленная за неправомерные действия со сведениями, отнесенными к коммерческой тайне.
19. Понятие банковской тайны. Виды информации, отнесенные к банковской тайне. Субъекты права на банковскую тайну.
20. Права и обязанности владельца банковской тайны. Ограничение прав субъектов.
21. Способы защиты права на банковскую тайну. Уголовная ответственность за незаконное получение и разглашение сведений, составляющих банковскую тайну.
22. Профессиональная тайна: понятие и виды. Краткая характеристика каждого вида.
23. Понятие служебной тайны Критерии (условия) охраноспособности. Виды служебных тайн. Права и обязанности субъектов права на служебную тайну. Способы защиты права на служебную тайну. Ответственность за разглашение сведений, составляющих служебную тайну.
24. Правовое регулирование взаимоотношений администрации и персонала в области защиты информации. Условия привлечения к дисциплинарной ответственности.
25. Правовое регулирование оперативно-розыскной деятельности. Особенности осуществления информационных процессов.

26. Правовые основы деятельности подразделений защиты информации на предприятии.
27. Частная детективная и охранная деятельность: понятие, субъекты и порядок регулирования.
28. Лицензирование при осуществление деятельности в сфере защиты информации.
29. Наивная криптография. Шифр Цезаря.
30. Идеальная криптосистема. Шифр Вернама.
31. Система обмена ключами Диффи и Хеллмана.
32. Шифр Шамира.
33. Шифр Эль-Гамаля.
34. Шифр RSA.
35. Электронная цифровая подпись. Схема протокола. Пример построения на основе шифра RSA.
36. Криптосистемы на эллиптических кривых. Основы арифметики на эллиптических кривых. Принцип построения криптосистем на эллиптических кривых.
37. Генераторы псевдо случайных чисел
38. Потоковые шифры. Примеры потоковых шифров.
39. Шифр RC4.
40. Блоковые шифры. Примеры блоковых шифров. Режимы функционирования блоковых шифров.
41. Схема построения потокового шифра на основе блокового шифра.
42. Теорема Шеннона.
43. Расстояние Хемминга. Вес Хэмминга. Код Хэмминнга.
44. Линейные коды. Проверочная матрица. Порождающая матрица. Теорема и связи проверочной и порождающей матриц.
45. Циклические коды.
46. Границы объемов кодов. Граница Хэмминга. Граница Синглтона.

Образец экзаменационного билета
(ФГБОУ ВО «КубГУ»)

Кафедра теоретической физики и компьютерный технологий
Направление подготовки 09.03.02 «Информационные системы и технологии» («Информационные системы и технологии»)
2018-2019 уч.год

Дисциплина «Информационная безопасность и защита информации»

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Шифр RC4.
2. Блоковые шифры. Примеры блоковых шифров. Режимы функционирования блоковых шифров.

Зав.кафедрой
теоретической
физики и компьютерный технологий д.ф-м.н., проф. Исаев В.А

Экзамен оценивается, исходя из следующих критериев:

«Отлично» – содержание ответа исчерпывает содержание билета. Студент демонстрирует как знание, так и понимание вопросов билета, а также знание основной и дополнительной литературы.

«Хорошо» – содержание ответа в основных чертах отражает содержание вопросов билета, но имеются некоторые пробелы и недочеты. Студент демонстрирует знание только основной литературы.

«Удовлетворительно» – содержание ответа в основных чертах отражает содержание билета, но имеются ошибки. Не все положения вопросов билета раскрыты полностью. Имеются фактические пробелы и не полное владение литературой. Нарушаются нормы философского языка; имеется нечеткость и двусмысленность письменной речи.

«Неудовлетворительно» – содержание ответа не отражает содержание билета. Имеются грубые ошибки, а также незнание ключевых определений и литературы. Письменные ответы на вопросы не написаны полностью; ответ не носит развернутого изложения билета.

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

Примерные темы рефератов

1. Особенности правовой охраны и защиты врачебной тайны.
2. Особенности правовой охраны и защиты тайны связи.
3. Особенности правовой охраны и защиты нотариальной тайны.
4. Особенности правовой охраны и защиты адвокатской тайны.
5. Особенности правовой охраны и защиты тайны страхования.
6. Особенности правовой охраны и защиты тайны исповеди и тайны усыновления.

Темы лабораторных работ

1. Концептуальные основы информационной безопасности предприятия
2. Анализ рисков информационной безопасности. Построение концепции информационной безопасности предприятия
3. Простейшие криптографические алгоритмы.

4. Программная реализация криптографических алгоритмов
5. Механизмы контроля целостности данных
6. Алгоритмы поведения вирусных и других вредоносных программ
7. Алгоритмы предупреждения и обнаружения вирусных угроз
8. Пакеты антивирусных программ
9. Выбор программно-аппаратного обеспечения для проектирования защищенной сети передачи данных

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

5.1 Основная литература:

1. Артемов, А.В. Информационная безопасность : курс лекций / А.В. Артемов ; Межрегиональная Академия безопасности и выживания. - Орел : МАБИВ, 2014. - 257 с. : табл., схем. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=42860

2. Спицын, В.Г. Информационная безопасность вычислительной техники : учебное пособие / В.Г. Спицын ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). - Томск : Эль Контент, 2011. - 148 с. : ил.,табл., схем. - ISBN 978-5-4332-0020-3 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=208694

3. Башлы, П.Н. Информационная безопасность : учебно-практическое пособие / П.Н. Башлы, Е.К. Баранова, А.В. Бабаш. - Москва : Евразийский открытый институт, 2011. - 375 с. - ISBN 978-5-374-00301-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=90539

5.2 Дополнительная литература:

1. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. – М.: Горячая линия-Телеком, 2012. – 288 с. Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=63235.

2. Нестеров С. А. Информационная безопасность: учебник и практикум для академического бакалавриата / С. А. Нестеров. — М.: Издательство Юрайт, 2017. — 321 с. — Режим доступа: www.biblio-online.ru/book/836C32FD-678E-4B11-8BFC-F16354A8AFC7.

3. Загинайлов, Ю.Н. Основы информационной безопасности: курс визуальных лекций : учебное пособие / Ю.Н. Загинайлов. - Москва ; Берлин : Директ-Медиа, 2015. - 105 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3947-4 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=362895

4. Прохорова, О.В. Информационная безопасность и защита информации : учебник / О.В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». - Самара : Самарский государственный архитектурно-строительный университет, 2014. - 113 с. : табл., схем., ил. - Библиогр. в кн. - ISBN 978-5-9585-0603-3 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=438331

5. Комплексное обеспечение информационной безопасности автоматизированных систем : лабораторный практикум / Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет» ; авт.-сост. М.А. Лапина, Д.М. Марков и др. - Ставрополь : СКФУ, 2016. - 242 с. : ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=458012

6. Пелешенко, В.С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления : учебное пособие / В.С. Пелешенко,

С.В. Говорова, М.А. Лапина ; Министерство образования и науки РФ, Федеральное государственное автономное образовательное учреждение высшего образования «Северо-Кавказский федеральный университет». - Ставрополь : СКФУ, 2017. - 86 с. : ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=467139

7. Информационные системы и технологии : научно-технический журнал / учредит. Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Государственный университет — учебно-научно-производственный комплекс» (Госуниверситет – УНПК) ; ред. сов. В.А. Голенков ; редкол. О.П. Архипов ; гл. ред. И.С. Константинов - Орел : Госуниверситет - УНПК, 2015. - № 5(91). - 152 с.: ил. - ISSN 2072-8964 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=446338

8. Инструментальный контроль и защита информации : учебное пособие / Н.А. Свинарев, О.В. Ланкин, А.П. Данилкин и др. ; Министерство образования и науки РФ, ФГБОУ ВПО «Воронежский государственный университет инженерных технологий». - Воронеж : Воронежский государственный университет инженерных технологий, 2013. - 192 с. : табл., ил. - Библиогр. в кн. - ISBN 978-5-00032-018-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=255905

9. Информационные системы и технологии : научно-технический журнал / учредит. Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Государственный университет — учебно-научно-производственный комплекс» (Госуниверситет – УНПК) ; ред. сов. В.А. Голенков ; редкол. О.П. Архипов ; гл. ред. И.С. Константинов - Орел : Госуниверситет - УНПК, 2013. - № 5(79). - 129 с.: ил. - ISSN 2072-8964 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=321627

10. Информационная безопасность и защита информации : сборник студенческих работ / отв. ред. А.Ю. Колябин. - Москва : Студенческая наука, 2012. - 1322 с. : ил.,табл., схем. - (Вузовская наука в помощь студенту). - ISBN 978-5-00046-137-2 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=227774

5.3. Периодические издания:

1. Вестник СПбГУ. Серия: Прикладная математика. Информатика. Процессы управления
2. Инфокоммуникационные технологии
3. Информатика и образование
4. Информатика. Реферативный журнал. ВИНИТИ
5. Информационное общество
6. Информационные ресурсы России
7. Информационные технологии
8. Компьютер Пресс
9. Нейрокомпьютеры: разработка, применение
10. Открытые системы.СУБД
11. Прикладная информатика
12. Проблемы передачи информации
13. Программирование
14. Программные продукты и системы

6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», в том числе современные профессиональные базы данных и информационные справочные системы, необходимые для освоения дисциплины (модуля).

Таблица 8

1. БД Web of Science - главный ресурс для исследователей по поиску и анализу научной литературы, охватывающей около 18000 научных журналов со всего мира. База данных международных индексов научного цитирования http://webofscience.com/
2. zbMATH - полная математическая база данных. Охватывает материалы с конца 19 века. zbMATH содержит около 4000000 документов из более 3000 журналов и 170000 книг по математике, статистике, информатике. https://zbmath.org/
3. БД Kaggle - это платформа для сбора и обработки данных. Является он-лайн площадкой для научного моделирования. https://www.kaggle.com/
4. База данных Научной электронный библиотеки eLIBRARY.RU https://elibrary.ru/
5. База данных Всероссийского института научной и технической информации (ВИНИТИ) РАН http://www2.viniti.ru/
6. «ЭЛЕКТРОННАЯ БИБЛИОТЕКА ДИССЕРТАЦИЙ» Российской Государственной Библиотеки (РГБ) – в настоящее время ЭБД содержит более 800 000 полных текстов диссертаций. https://dvs.rsl.ru
7. Портал открытых данных Российской Федерерации https://data.gov.ru
8. База открытых данных Министерства труда и социальной защиты РФ https://rosmintrud.ru/opendata
9. Федеральный портал единое окно доступа к информационным ресурсам - http://window.edu.ru/
10. Российский фонд фундаментальных исследований предоставляет доступ к информационным наукометрическим базам данных и полнотекстовым научным ресурсами издательств Springer Nature и Elsevier - http://www.rfbr.ru/rffi/ru
11. Федеральный портал "Информационно-коммуникационные технологии в образовании" - http://www.ict.edu.ru/
12. «Лекториум ТВ» – видеолекции ведущих лекторов России. Лекториум – on-line – библиотека, где ВУЗы и известные лектории России презентуют своих лучших лекторов. Доступ к материалам свободный и бесплатный - http://www.lektorium.tv.

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

Подготовка к лекционному занятию включает выполнение всех видов заданий, рекомендованных к каждой лекции, т.е. задания выполняются еще до лекционного занятия по соответствующей теме.

В ходе лекционных занятий необходимо вести конспектирование учебного материала, обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Необходимо задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций. Целесообразно дорабатывать свой конспект лекции, делая в нем соответствующие записи из литературы, рекомендованной преподавателем и предусмотренной учебной программой.

Практические занятия позволяют развивать у студентов творческое теоретическое мышление, умение самостоятельно изучать литературу, анализировать практику; учат четко формулировать мысль, вести дискуссию, то есть имеют исключительно важное значение в развитии самостоятельного мышления.

Преподаватель должен прогнозировать затруднения, которые могут возникнуть у студентов при самостоятельном изучении и усвоении учебного материала и предусмотреть оперативную консультацию по любому вопросу. Если возникают затруднения по одному и тому же материалу (вопросу) у многих студентов, то желательно провести групповую консультацию. Консультации должны быть краткими: групповая - 2-

3 мин., индивидуальная - 1-2 мин. Глубину и качество усвоения учебного материала необходимо непрерывно отслеживать при проведении текущего контроля знаний.

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, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

Методические рекомендации по подготовке рефератов и докладов.

Тема выбирается из числа предложенных преподавателем дисциплины или может быть определена самостоятельно по рекомендации научного руководителя. Реферат должен включать в себя оглавление, введение, основную часть, заключение, биографические справки об упоминаемых в тексте учёных и подробный библиографический список, составленный в соответствии со стандартными требованиями к оформлению литературы, в том числе к ссылкам на электронные ресурсы. Работа должна носить самостоятельный характер, в случае обнаружения откровенного плагиата (дословного цитирования без ссылок) реферат не засчитывается. Сдающий реферат студент должен продемонстрировать умение работать с литературой, отбирать и систематизировать материал, увязывать его с существующими теориями и известными фактами.

Во введении обосновывается актуальность выбранной темы, определяются цели и задачи реферата, приводятся характеристика проработанности темы в историко-математической литературе и краткий обзор использованных источников.

В основной части, разбитой на разделы или параграфы, излагаются основные факты, проводится их анализ, формулируются выводы (по разделам). Необходимо охарактеризовать современную ситуацию, связанную с рассматриваемой тематикой.

Заключение содержит итоговые выводы и, возможно, предположения о перспективах проведения дальнейших исследований по данной теме.

Биографические данные можно оформлять сносками или в качестве приложения к работе.

Список литературы может быть составлен в алфавитном порядке или в порядке цитирования, в полном соответствии с государственными требованиями к библиографическому описанию. Ссылки в тексте должны быть оформлены также в соответствии со стандартными требованиями (с указанием номера публикации по библиографическому списку и страниц, откуда приводится цитата).

Подготовку реферата рекомендуется начинать с библиографического поиска и составления библиографического списка, а также подготовки плана работы. Каждый из намеченных пунктов плана должен опираться на различные источники, при этом желательно провести сравнительный анализ как результатов, полученных разными специалистами, так и взглядов на эту темы различных специалистов в области истории науки. Необходимо выявить предпосылки и отметить последствия анализируемых теорий, отметить философские и методологические особенности. Текст реферата должен быть связным, недопустимы повторения, фрагментарный пересказ разрозненных сведений и фактов.

Оформление реферата должно быть аккуратным, при использовании редакторов LaTeX или MS WORD рекомендуется шрифт 12 пт. Ориентировочный объём – не менее 15 страниц, при этом не допускается его искусственное увеличение за счет междустрочных интервалов. Титульный лист готовится в соответствии с требованиями, предъявляемыми к оформлению титульных листов дипломных работ.

Для доклада необходимо подготовить слайды презентации – например, средствами Microsoft Office PowerPoint – по материалам реферата. К слайдам прилагается doc-файл

текста выступления. Перед выступлением на занятиях содержание доклада и слайдов необходимо согласовать с преподавателем.

Рекомендации по оцениванию лабораторных работ

В целях закрепления практического материала и углубления теоретических знаний по разделам дисциплины «Информационная безопасность и защита информации» предполагается выполнение лабораторных работ, что позволяет углубить процесс познания, раскрыть понимание прикладной значимости осваиваемой дисциплины. Комплект заданий репродуктивного уровня для выполнения на лабораторных занятиях, позволяющих оценивать и диагностировать знание фактического материала (базовые понятия, алгоритмы, факты) и умение правильно использовать специальные термины и понятия, распознавание объектов изучения в рамках определенного раздела дисциплины.

Критерии оценки лабораторных работ

Оценка	Критерии оценивания
5 баллов	Задание выполнено полностью, в представленном отчете обоснованно получено правильное выполненное задание.
4 балла	Задание выполнено полностью, но нет достаточного обоснования или при верном решении допущена незначительная ошибка, не влияющая на правильную последовательность рассуждений.
3 балла	Задания выполнены частично.
2 балла	Задание не выполнено.

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

8.1 Перечень информационных технологий.

– Проверка заданий и консультирование посредством электронной почты и популярных соц.сетей.

– Использование электронных презентаций при проведении лекционных занятий.

- Разбор готовых программных проектов на практических занятиях.

8.2 Перечень необходимого лицензионного программного обеспечения.

1. Операционная система MS Windows версии XP, 7,8,10;
2. Пакет офисных программ Microsoft Office 2010;
3. MS Visio, MS Visual Studio;
4. Oracle Virtual Box.

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

№	Вид работ	Материально-техническое обеспечение дисциплины (модуля) и оснащенность
1.	*Лекционные занятия*	Лекционная аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) и соответствующим программным обеспечением (ПО) для воспроизведения файлов формата jpg и avi, достаточным количеством посадочных мест. 300, 114, 209, 201 корп. С.

2.	*Семинарские занятия*	Не предусмотрено
3.	*Лабораторные занятия*	Лаборатория, укомплектованная специализированной мебелью и техническими средствами обучения. 207, 212, 213 корп. С.
4.	*Курсовое проектирование*	Не предусмотрено
5.	*Групповые (индивидуальные) консультации*	Аудитория для проведения групповых (индивидуальных) занятий, оснащенная доской и комплектом учебной мебели. 212, 213, 207 корп. С.
6.	*Текущий контроль, промежуточная аттестация*	Аудитория для текущего контроля и промежуточной аттестации студентов, оснащенная компьютерной техникой с возможностью подключения к сети “Интернет”, с соответствующим программным обеспечением в режиме подключения к терминальному серверу, с программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета. 114, 212, 230 корп. С.
7.	*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. 208 корп. С.