Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Ворошилова Ольга Леонидовна
Должность: декан ФЛиМК
Дата подписания: 18.09.2022 18:26:08
Уникальный программный ключ:
abd894de8ff3e434f187dcddc5d14b3be82fda3f663e010c359e4ba6bb821c5e

Аннотация к рабочей программе дисциплины «Информационная безопасность и защита информации»

Цель преподавания дисциплины:

дать систематический обзор современных методов защиты информации и обеспечения компьютерной безопасности при реализации процессов ввода, вывода, передачи, обработки, накопления и хранения информации.

Задачи изучения дисциплины:

– изучить и освоить принципы современных методов защиты информации и их построения,

– рассмотреть перспективные направления развития существующих систем.

Компетенции, формируемые в результате освоения дисциплины:

– ОПК-1 — способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности, использовать различные источники информации по объекту туристского продукта; - способностью обрабатывать и интерпретировать с использованием базовых знаний математики и

информатики данные, необходимые для осуществления проектной деятельности в туризме (ПК-2).

Разделы дисциплины:

– Цель и задачи дисциплины, ее роль и место в общей системе подготовки специалиста.

– Защита информации и информационная безопасность как важный фактор политической и экономической составляющих национальной безопасности.

– Программа информационной безопасности России и пути ее реализации.

– Проблемы и методы защиты информации.

– Информационная безопасность.

– Проблемы защиты информации в компьютерных системах.

– Защита информации при реализации информационных процессов ввода, вывода, передачи, обработки, накопления и хранения информации.

– Организационное обеспечение информационной безопасности.

– Математические и методологические средства защиты информации.

– Компьютерные средства реализации защиты в информационных системах.

– Физический, сетевой, транспортный и прикладной уровни защиты информации.

– Обзор стандартов в области защиты информации.

– Методы и средства защиты локальной рабочей станции.

– Защита в локальных сетях.

МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
Декан факультета
Лингвистики и межкультурной
(наименование ф-та полностью)
коммуникации
О.Л. Ворошилова
(подпись, инициалы, фамилия)
«____» _____ 20___ г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность и защита информации

направление подготовки (специальность) *43.03.03*
(шифр согласно ФГОС
Гостиничное дело
и наименование направления подготовки (специальности)

Ресторанная деятельность
наименование профиля, специализации или магистерской программы

форма обучения *заочная*
очная, очно-заочная, заочная

Курск – 20*16*

Рабочая программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования направления подготовки *43.03.03 – «Гостиничное дело»* и на основании учебного плана направления подготовки *43.03.03 – «Гостиничное дело»*, одобренного Учёным советом университета, протокол № 5 «30» 01 2017 г.

Рабочая программа обсуждена и рекомендована к применению в учебном процессе для обучения студентов по направлению подготовки *43.03.03 – «Гостиничное дело»* на заседании кафедры информационной безопасности.

«1» февраля 2017г. Протокол № 9

И.о. зав. кафедрой ИБ Таныгин М.О.

Разработчик программы,
доцент кафедры ИБ Марухленко А.Л.

Согласовано: на заседании кафедры истории и социально-культурного сервиса №___ «____» _____ 201__ г.

Зав. кафедрой Горюшкина Н.Е.

Директор научной библиотеки Макаровская В.Г.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 43.03.03 «Гостиничное дело», одобренного Ученым советом университета протокол №1«22»09 2017г.на заседании кафедры _____

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____ Таныгин М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 43.03.03 «Гостиничное дело», одобренного Ученым советом университета протокол №5«30»01 2017г.на заседании кафедры ИБ, протокол №12 от 29.06.18г.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____ Таныгин М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 43.03.03 «Гостиничное дело», одобренного Ученым советом университета протокол №1«1»06 201г.на заседании кафедры [illegible]

(наименование кафедры, дата, номер протокола)

Зав. кафедрой ____________________________

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 43.03.03 «Гостиничное дело», одобренного Ученым советом университета протокол №_«__»___20_г.на заседании кафедры____________________________

(наименование кафедры, дата, номер протокола)

Зав. кафедрой ____________________________

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 43.03.03 «Гостиничное дело», одобренного Ученым советом университета протокол №_«__»___20_г.на заседании кафедры____________________________

(наименование кафедры, дата, номер протокола)

Зав. кафедрой ____________________________

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 43.03.03 «Гостиничное дело», одобренного Ученым советом университета протокол №_«__»___20_г.на заседании кафедры____________________________

(наименование кафедры, дата, номер протокола)

Зав. кафедрой ____________________________

1. Цель и задачи дисциплины. Перечень планируемых результатов обучения, соотнесённых с планируемыми результатами освоения образовательной программы

1.1. Цель дисциплины

Дисциплина «Информационная безопасность и защита информации» изучается с целью ознакомления студентов с современным состоянием теории безопасности информационных систем, правовым регулированием в области защиты информации, принципами организации аппаратно-программных способов защиты информации в организациях и предприятиях различных направлений деятельности и различных форм собственности.

1.2. Задачи дисциплины

Основными задачами изучения учебной дисциплины являются приобретение студентами познаний в области:

– защиты безопасности;

– информационной безопасности – сравнительно молодой, быстро развивающейся области информационных технологий (словосочетание «информационная безопасность» в разных контекстах может иметь различный смысл);

– защищенности национальных интересов в информационной сфере;

– правильного подхода к проблемам информационной безопасности, который начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем (ИС).

1.3. Перечень планируемых результатов обучения, соотнесённых с планируемыми результатами освоения образовательной программы

Обучающиеся должны **знать**:

– основные принципы системы информационной безопасности и защиты информации

– последние тенденции соответствующие требованиям потребителя

уметь:

– принимать управленческие решения для решения профессиональных задач

– предоставить готовый гостиничный продукт с помощью новейших технологий

владеть:

– навыками быстрого поиска и анализа полученной информации

– навыками разработки и предоставления гостиничного продукта

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– способностью анализировать физические явления и процессы для решения профессиональных задач (ОПК-1);

– готовностью к разработке и предоставлению гостиничного продукта, в том числе в соответствии с требованиями потребителя, на основе новейших информационных и коммуникационных технологий (ПК-2)

2. Указание места дисциплины в структуре образовательной программы

«Информационная безопасность и защита информации» (Б1.В.ДВ.4.1) является дисциплиной по выбору вариативной части учебного плана направления подготовки 43.03.03 «Гостиничное дело». Изучается на 2 курсе в 3 семестре.

3. Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоёмкость (объём) дисциплины составляет 5 зачётных единиц, 180 академических часов.

Таблица 3.1 – Объём дисциплины по видам учебных занятий

Общая трудоемкость дисциплины	180
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	8,15
Лекции	4
лабораторные занятия	0
практические занятия	4
Экзамен	0,15
зачет	не предусмотрен
курсовая работа (проект)	не предусмотрена
расчетно-графическая (контрольная) работа	не предусмотрена
Аудиторная работа (всего):	8
в том числе:	
лекции	4
лабораторные занятия	0
практические занятия	4
Самостоятельная работа обучающихся (всего)	163
Контроль/экз (подготовка к экзамену)	9

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

4.1 Содержание дисциплины

Таблица 4.1 – Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел (тема) дисциплины	Содержание
1.	Введение в информационную безопасность	Информационная сфера (среда). Целостность Доступность. Конфиденциальность. Основные принципы обеспечения информационной безопасности. Системность подхода. Комплексность подхода. Принцип разумной достаточности.
2.	Понятие защищенности в автоматизированных системах	Понятие защищенности. Меры и средства защиты информации
3.	Основы законодательства РФ в области информационной безопасности и защиты информации	Федеральный закон «Об информации, информационных технологиях и о защите информации». государственная тайна. следующая система обозначения сведений: «Особой важности», «Совершенно секретно», «Секретно».
4.	Конфиденциальная информация и ее защита	Коммерческая тайна. Служебная тайна. Профессиональная тайна. Персональные данные
5.	Лицензирование и сертификация в области обеспечения безопасности информации	Лицензирование. Организационное обеспечение информационной безопасности. Организационные (административные) средства защиты.
6.	Технические средства обеспечения информационной безопасности	Основные технические средства. Вспомогательные технические средства и системы
7.	Электромагнитные каналы утечки информации	Побочные электромагнитные излучения ТСПИ. Побочные электромагнитные излучения на частотах работы высокочастотных генераторов ТСПИ. Паразитная генерация (побочные электромагнитные излучения, возникающие вследствие паразитной генерации в элементах ТСПИ)
8.	Электрические каналы утечки информации	Причинами возникновения электрических каналов утечки информации. Способы и средства подавления электронных устройств перехвата речевой информации
9.	Угроза безопасности информации АСОД и субъектов информационных отношений	Угроза интересов субъекта информационных отношений. Классификация угроз безопасности. Классификация каналов проникновения в систему и утечки информации. При контактном НСД. При бесконтактном НСД. Неформальная модель нарушителя в АСОД

Таблица 4.2 – Содержание дисциплины и ее методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		лек. час	№ лб	№ пр.			
1	2	3	4	5	6	7	8
1	Основы законодательства РФ в области информационной безопасности и защиты информации	2		1	О-4,5 Д-3-6	КО(1-2)	ОПК-1 ПК-2
2	Технические средства обеспечения информационной безопасности	2		2	О-2,3, Д-3-5	КО(3-4)	ОПК-1 ПК-2

К – контрольная работа, С – собеседование, КО – контрольный опрос

4.2. Лабораторные работы и (или) практические занятия

4.2.1. Практические занятия

Таблица 4.3. – Практические занятия

№	Наименование практического занятия	Компетенции	Объем, час.
1	2	3	4
1	Практическая работа №1 «Алгоритм шифрования RSA»	ОПК-1 ПК-2	2
2	Практическая работа №2 «Алгоритм шифрования Эль – Гамаля»	ОПК-1 ПК-2	2
Итого			4

4.3. Самостоятельная работа студентов (СРС)

Таблица 4.4 – Самостоятельная работа студентов

№	Наименование раздела учебной дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1	2	3	4
1.	Введение в информационную безопасность	1-2 недели	16
2.	Понятие защищенности в автоматизированных системах	3-4 недели	16
3.	Основы законодательства РФ в области информационной безопасности и защиты информации	5-6 недели	16
4.	Конфиденциальная информация и ее защита	7-8 недели	16
5.	Лицензирование и сертификация в области обеспечения безопасности информации	9-10 недели	16
6.	Технические средства обеспечения информационной безопасности	11-12 недели	16
7.	Электромагнитные каналы утечки информации	13-14	16

		недели	
8.	Электрические каналы утечки информации	15-16 недели	16
9.	Угроза безопасности информации АСОД и субъектов информационных отношений	17-19 недели	16
10.	Подготовка к экзамену	1-18 недели	19
Итого			163

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

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное Правилами внутреннего распорядка работников.

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

– библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с данной РПД;

– имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

– путем обеспечения доступности всего необходимого учебно-методического и справочного материала;

– путем предоставления сведений о наличии учебно-методической литературы, современных программных средств;

– путем разработки вопросов к экзамену, методических указаний к выполнению лабораторных и практических работ.

типографией университета:

– путем помощи авторам в подготовке и издании научной, учебной, учебно-методической литературы;

– путем удовлетворения потребностей в тиражировании научной, учебной, учебно-методической литературы.

6. Образовательные технологии

В соответствии с требованиями ФГОС и Приказа Министерства образования и науки РФ от 05 апреля 2017 г. №301 реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения

занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков студентов. Удельный вес занятий, проводимых в интерактивных формах, составляет 24.9% от аудиторных занятий согласно УП. Средствами промежуточного контроля успеваемости студентов являются защита лабораторных работ, опросы на практических занятиях по темам лекций.

Таблица 6.1 – Интерактивные образовательные технологии, используемые при проведении аудиторных занятий

№	Наименование раздела	Используемые интерактивные образовательные технологии	Объём, час.
1.	Основные законы в области защиты информации. Лицензирование в области защиты информации. (лекция)	Групповое обсуждение с элементами дискуссии рассматриваемых на лекции вопросов	2
	Итого		2

7. Фонд оценочных средств для проведения промежуточной аттестации

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Таблица 7.1 – Этапы формирования компетенций

Код и содержание компетенции	Этапы формирования компетенций и дисциплины (модули), при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
способностью анализировать физические явления и процессы для решения профессиональных задач (ОПК-1)	Информатика Информационная безопасность и защита информации Интернет-технологии	Практика по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно- исследовательской деятельности	
готовностью к разработке и предоставлению гостиничного продукта, в том числе в соответствии с требованиями	Информационная безопасность и защита информации Интернет-технологии	Технологии гостиничной деятельности Практика по получению профессиональных умений и опыта профессиональной деятельности	Организация производства и обслуживания в ресторанной деятельности

потребителя, на основе новейших информационных и коммуникационных технологий (ПК-2)			

7.2. Описание показателей и критериев оценивания компетенций на раз- личных этапах их формирования, описание шкал оценивания

Таблица 7.2 – Критерии и шкала оценивания компетенций

Код компетенции / Этап	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно»)	Продвинутый уровень («хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
ОПК-1 начальный	1.Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п. 1.3 РПД 2.Качество освоенных обучающимся знаний, умений, навыков 3.Умение применять знания, умения, навыки в типовых и нестандартных ситуациях	**Знать**: основные принципы законы физические явления и процессы **Уметь**: анализировать **Владеть**: навыками применения законов в конкретной жизненной ситуации	**Знать**: основные принципы системы информационной безопасности **Уметь**: отыскать необходимую информацию **Владеть**: навыками анализировать полученную информацию	**Знать**: основные принципы системы информационной безопасности и защиты информации **Уметь**: принимать управленческие решения для решения профессиональных задач **Владеть**: навыками быстрого поиска и анализа полученной информации
ПК-2 начальный	1.Доля освоенных обучающимся знаний, умений,	**Знать**: основные информационных и коммуникационных технологий	**Знать**: основные принципы системы информационных и коммуникационных технологий	**Знать**: последние тенденции соответствующие требованиям потребителя

	навыков от общего объема ЗУН, установленных в п. 1.3 РПД 2.Качество освоенных обучающимся знаний, умений, навыков 3.Умение применять знания, умения, навыки в типовых и нестандартных ситуациях	**Уметь**: находить необходимую информацию **Владеть**: предоставления гостиничного продукта	**Уметь**: анализировать полученную информацию **Владеть**: навыками освоения новейших информационных и коммуникационных технологий	**Уметь**: предоставить готовый гостиничный продукт с помощью новейших технологий **Владеть**: навыками разработки и предоставлению гостиничного продукта

7.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Таблица 7.3 – Паспорт комплекта оценочных средств для текущего контроля

№ п/п	Раздел (тема) дисциплины	Код компетенции (или её части)	Технология формирования	Оценочные средства	Описание шкал оценивания
				наименование	
1	2	3	4	5	6
1	Введение в информационную безопасность	ОПК-1 ПК-2	Лекция, практические занятия, СРС	Собеседование	В соответствии с таблицей 7.2
2	Понятие защищенности в автоматизированных системах	ОПК-1 ПК-2	Лекция, практические занятия, СРС	Контрольный опрос	В соответствии с таблицей 7.2

3	Основы законодательства РФ в области информационной безопасности и защиты информации	ОПК-1 ПК-2	Лекция, практические занятия, СРС	Контрольный опрос	В соответствии с таблицей 7.2
4	Конфиденциальная информация и ее защита	ОПК-1 ПК-2	Лекция, практические занятия, СРС	Собеседование	В соответствии с таблицей 7.2
5	Лицензирование и сертификация в области обеспечения безопасности информации	ОПК-1 ПК-2	Лекция, практические занятия, СРС	Собеседование	В соответствии с таблицей 7.2
6	Технические средства обеспечения информационной безопасности	ОПК-1 ПК-2	Лекция, практические занятия, СРС	Собеседование	В соответствии с таблицей 7.2
7	Электромагнитные каналы утечки информации	ОПК-1 ПК-2	Лекция, практические занятия, СРС лабораторная работа	Собеседование	В соответствии с таблицей 7.2
8	Электрические каналы утечки информации	ОПК-1 ПК-2	Лекция, практические занятия, СРС	Контрольный опрос	В соответствии с таблицей 7.2
9	Угроза безопасности информации АСОД и субъектов информационных отношений	ОПК-1 ПК-2	Лекция, практические занятия, СРС	Контрольная работа	В соответствии с таблицей 7.2

Примеры типовых контрольных заданий для текущего контроля

Примеры контрольного опроса

1. Определение информации.
2. Компьютерные вирусы, их классификация.
3. Виды угроз информации.
4. Что такое алгоритм шифрования.
5. Криптостойкость.

6. Алгоритм RSA.
7. Аутентификация и авторизация.

Примеры вопросов для собеседования

1. Общая характеристика электромагнитного канала утечки информации
2. Сетевые атаки. Системы обнаружения атак
3. Виды конфиденциальной информации
4. Политика информационной безопасности
5. Определение информационной безопасности

Промежуточная аттестация по дисциплине проводится в форме экзамена. Экзамен проводится в форме письменного экзамена. Для текущего контроля используются тестовые задания - закрытой (с выбором одного или нескольких правильных ответов)

Умения, навыки и компетенции проверяются с помощью задач (ситуационных, производственных или кейсового характера) и различного вида конструкторов. Часть умений, навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

7.4. Рейтинговый контроль изучения учебной дисциплины

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

– Положение П 02.016–2015 «О балльно-рейтинговой системе оценки качества освоения образовательных программ»;

– методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля* по дисциплине в рамках действующей в университете балльно-рейтинговой системы применяется следующий порядок начисления баллов:

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
1	2	3	4	5
Практическая работа №1 «Алгоритм шифрования RSA»	0	Выполнил, но «не защитил»	6	Выполнил и «защитил»
Практическая работа №2 «Алгоритм шифрования Эль – Гамаля»	0	Выполнил, но «не защитил»	7	Выполнил и «защитил»
СРС	0		13	

1	2	3	4	5
Итого	0		26	
Посещаемость	0		14	
Экзамен	0		60	
Итого	0		100	

Для промежуточной аттестации, проводимой в форме тестирования, используется следующая методика оценивания знаний, умений, навыков и (или) опыта деятельности. В каждом варианте КИМ -16 заданий (15 вопросов и одна задача)

Каждый верный ответ оценивается следующим образом:

- задание в закрытой форме–3 балла,
- задание в открытой форме–3 балла,
- задание на установление правильной последовательности–3 балла,
- задание на установление соответствия–3 балла,
- решение задачи – 15 баллов.

Максимальное количество баллов за тестирование - 60 баллов.

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

8.1. Основная учебная литература

1) Технологии защиты информации в компьютерных сетях. Межсетевые экраны и интернет-маршрутизаторы [Текст] : учебное пособие / Е. А. Богданова [и др.]. - Москва : Национальный Открытый Университет "ИНТУИТ", 2013. - 743 с. - (Основы информационных технологий). - ISBN 978-5-9556-01 42-7

2) Ищейнов, Вячеслав Яковлевич. Защита конфиденциальной информации [Текст] : учебное пособие / В. Я. Ищейнов, М. В. Мецатунян. - Москва : Форум, 2013. - 256 с. : ил. - (Высшее образование). - ISBN 978-5-91134-3 36-1.

3) Спеваков, А. Г. Основы правового обеспечения информационной безопасности [Текст] : учебное пособие / А. Г. Спеваков, А. П. Фисун ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2013 - .Ч. 1. - 150 с. : ил., табл. - Имеется электрон. аналог. - Библиогр.: с. 137-149. - ISBN 978-5-7681-08 57-1.

4) Загинайлов, Ю. Н. Теория информационной безопасности и методов за-щиты информации [Электронный ресурс] : учеб. пособие / Ю. Н. Загинайлов. – М . : Директ-Медиа, 2015. – 253 с. Режим доступа : http://biblioclub.ru/index.php?page=book_red&id=276557

8.2. Дополнительная литература

1) Организационно-правовое обеспечение информационной безопасности [Текст] : учебное пособие / под ред. А. А. Стрельцова. - М. : Академия, 2008. - 256 с. - (Высшее профессиональное образование). - ISBN 978-5-7695-42 40-4.

2) Романов, О. А. Организационное обеспечение информационной безопасности [Текст] : учебник / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М. : Академия, 2008. - 192 с. - (Высшее профессиональное образование). - ISBN 978-5-7695-42 72-5

3) Рябко, Борис Яковлевич. Основы современной криптографии и стенографии [Текст] : монография / Б. Я. Рябко, А. Н. Фионов. - М. : Горячая линия-Телеком, 2010. - 232 с. : ил. - ISBN 978-5-9912-01 50-6

4) Спицин, В. Г. Информационная безопасность вычислительной техники [Электронный ресурс] : учебное пособие / Спицин В. Г. - Томск : Эль-Контент, 2011. - 148 с. - Режим доступа : http://biblioclub.ru/index.php?page=book_red&id=208694

8.3. Перечень методических указаний

1) Алгоритм шифрования RSA: методические указания к выполнению практических работ по дисциплинам: «Защита информации», «Информационная безопасность» / Юго-Зап. гос. ун-т; сост. А.Л. Марухленко. Курск, 2017.

2) Алгоритм шифрования Эль – Гамаля: методические указания к выполнению практических работ по дисциплинам: «Защита информации», «Информационная безопасность» / Юго-Зап. гос. ун-т; сост. А.Л. Марухленко. Курск, 2017.

8.4. Другие учебно-методические материалы

Научно-технические журналы в библиотеке университета:
Информационная безопасность
Защита информации
Бюллетень Министерства труда и социального законодательства РФ
Нормативно-правовые акты РФ

9. Перечень ресурсов информационно – телекоммуникационной сети Интернет, необходимых для освоения дисциплины

1) Федеральная служба безопасности [официальный сайт]. Режим доступа: http://www.fsb.ru/.

2) Федеральная служба по техническому и экспортному контролю [официальный сайт]. Режим доступа: http://fstec.ru/

3) Электронная библиотека ЮЗГУ (http:// http://lib.swsu.ru)

4) Электронно-библиотечная система Университетская библиотека онлайн (https://biblioclub.ru)

10. Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Информационная безопасность и защита информации» являются лекции и лабораторные занятия. Студент не имеет права пропускать занятия без уважительных причин.

На лекциях излагаются и разъясняются основные понятия темы, связанные с ней теоретические и практические проблемы, даются рекомендации для самостоятельной работы. В ходе лекции студент должен внимательно слушать и конспектировать материал.

Изучение наиболее важных тем или разделов дисциплины завершают лабораторные занятия, которые обеспечивают: контроль подготовленности студента; закрепление учебного материала; приобретение опыта устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

Лабораторному занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

По согласованию с преподавателем или по его заданию студенты готовить рефераты по отдельным темам дисциплины, выступать на занятиях с докладами. Основу докладов составляет, как правило, содержание подготовленных студентами рефератов.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, собеседования, защиты отчетов по лабораторным работам, а также по результатам докладов.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Проектирование защищённых телекоммуникационных систем»: конспектирование учебной литературы и лекции, составление словарей понятий и терминов и т. п.

В процессе обучения преподаватели используют активные формы работы со студентами: чтение лекций, привлечение студентов к творческому процессу на лекциях, промежуточный контроль путем отработки студентами пропущенных лекции, участие в групповых и индивидуальных консультациях (собеседовании). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы составляет значительную часть самостоятельной работы студента. Это

большой труд, требующий усилий и желания студента. В самом начале работы над книгой важно определить цель и направление этой работы. Прочитанное следует закрепить в памяти. Одним из приемов закрепление освоенного материала является конспектирование, без которого немыслима серьезная работа над литературой. Систематическое конспектирование помогает научиться правильно, кратко и четко излагать своими словами прочитанный материал.

Самостоятельная работа студентов включает в себя изучение материалов дисциплины по записям лекций и учебникам, выполнение домашних заданий, оформление отчетов по лабораторным работам и практическим занятиям, подготовку рефератов по заданным темам, а также подготовку к зачету и экзамену. Вся эта работа планируется самим студентом по рекомендациям преподавателя.

Студенты, не имеющие опыта и считающие, что можно работать без плана, запускают занятия и, будучи не в состоянии нагнать пропущенное, перестают понимать лекции, не справляются с решением задач на лабораторных и практических занятиях.

Оценка результативности самостоятельной работы студентов обеспечивается контрольными опросами и собеседованиями со студентами и проверкой выполнения заданий по преподавателя.

Рекомендуется следующий порядок работы студента. Сначала выполняется наиболее трудная ее часть: изучение учебного материала по записям лекций, прослушанных в этот же день. Прочтя свою запись и дополнив ее тем, что еще свежо в памяти, студент обращается к учебнику по дисциплине или к электронному ресурсу. Рекомендуется делать выписки из источников информации на свободных страницах конспекта. В процессе проработки материала отмечаются неясные стороны изучаемой темы и формулируются вопросы, которые следует задать преподавателю.

Наилучшего результата достигают те студенты, которые предварительно знакомятся с материалом по теме предстоящих занятий. Благодаря этому студенты будут осознанно и критически относиться к изложению лекции и воспримут ее с большим “коэффициентом полезного действия”.

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

- Libreoffice операционная система Windows
- глобальная сеть Internet
- Антивирус Касперского (или ESETNOD)

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

Учебная аудитория для проведения занятий лекционного типа и лаборатории кафедры информационной безопасности, оснащенные учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска. Компьютеры (12 шт) CPU AMD-Phenom, ОЗУ 16 GB, HDD 2 Tb, монитор Aok 21”. Проекционный экран на штативе; Мультимедиацентр: ноут- букASUSX50VLPMD-T2330/14"/1024Mb/160Gb/сумка/ проектор inFocusIN24+

13. Лист дополнений и изменений, внесенных в рабочую программу дисциплины

Номер изменения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего изменения
	Изменённых	заменённых	аннулированных	новых			