МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
Декан факультета
Экономики и менеджмента
(наименование ф-та полностью)

Т.Ю. Ткачева
(подпись, инициалы, фамилия)
«*01*» *марта* 20*17* г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность

направление подготовки (специальность) *38.05.01*
(шифр согласно ФГОС
Экономическая безопасность
и наименование направление подготовки (специальности)

Экономико-правовое обеспечение экономической безопасности
наименование профиля, специализации или магистерской программы

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

Курск – 20*17*

Рабочая программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по специальности 38.03.05 «Экономическая безопасность» и на основании учебного плана специальности 38.05.01 «Экономическая безопасность», одобренного Учёным советом университета, протокол 6 «27» февраля 2017 г.

Рабочая программа обсуждена и рекомендована к применению в образовательном процессе для обучения студентов по специальности 38.05.01 «Экономическая безопасность» на заседании кафедры информационной безопасности «28» февраля 2017 г. Протокол № 10

И.о. зав. кафедрой ИБ Таныгин М.О.

Разработчик программы
доцент кафедры ИБ Марухленко А.Л.

Согласовано: на заседании кафедры экономической безопасности и налогообложения протокол №10 «01» марта 2017 г.

И.о. зав. кафедрой Афанасьева Л.В.

Директор научной библиотеки Макаровская В.Г.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана специальности 38.05.01 «Экономическая безопасность», одобренного Ученым советом университета протокол №6 «27» февраля 2017 г. на заседании кафедры ИБ 28 августа 2017 г. протокол № 1

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана специальности 38.05.01 «Экономическая безопасность», одобренного Ученым советом университета протокол №5 «30» 01 2018 г. 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 специальности 38.05.01

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана специальности 38.05.01 – «Экономическая безопасность», одобренного Ученым советом университета протокол №5 «30» 01 2019 г. на заседании кафедры ИБ, протокол № 12 от 27.06.19

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____ / Ткачёв М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана специальности 38.05.01 – «Экономическая безопасность», одобренного Ученым советом университета протокол №9 «29» 03 2019 г. на заседании кафедры Информационной безопасности протокол №1 от 31.08.2020

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____ / Ткачёв М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана специальности 38.05.01 – «Экономическая безопасность», одобренного Ученым советом университета протокол №7 «25» 02 2020 г. на заседании кафедры ИБ, протокол № 11 от 28.06.21г

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____ / Ткачёв М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана специальности 38.05.01 – «Экономическая безопасность», одобренного Ученым советом университета протокол №7 «25» 02 2020 г. на заседании кафедры ИБ, протокол № 11 от 30.06.2022 г

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____ / Ткачёв М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана специальности 38.05.01 – «Экономическая безопасность», 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» 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 экономической безопасности

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– способность применять основные закономерности создания и принципы функционирования систем экономической безопасности хозяйствующих субъектов (ОПК-3)

– способность соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности (ПК-20)

2. Указание места дисциплины в структуре образовательной программы

«Информационная безопасность» представляет дисциплину с индексом Б1.В.ДВ.4 вариативной части базового цикла учебного плана по специальности 38.05.01 «Экономическая безопасность», изучаемую на 2 курсе в 4 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 2 зачётных единиц, 72 академических часа.

Таблица 3.1 – Объём дисциплины по видам учебных занятий

Общая трудоемкость дисциплины	72
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	36,1
Лекции	18
лабораторные занятия	0
практические занятия	18
Экзамен	не предусмотрен
зачет	0,1
курсовая работа (проект)	не предусмотрена
расчетно-графическая (контрольная) работа	не предусмотрена
Аудиторная работа (всего):	54
в том числе:	
лекции	18
лабораторные занятия	0
практические занятия	18
Самостоятельная работа обучающихся (всего)	35,9
Контроль/экз (подготовка к экзамену)	

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)

№	Раздел (тема)	Содержание

п/п	дисциплины	
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	Учебно-методические материалы		Формы текущего контроля успеваемости *(по неделям семестра)*		Компетенции
		лек. час	№ пр.			
1	2	3	4	6	7	8

№ п/п	Раздел (тема) дисциплины	Учебно-методические материалы		Формы текущего контроля успеваемости *(по неделям семестра)*		Компетенции
		лек. час	№ пр.			
1	2	3	4	6	7	8
1	Введение в информационную безопасность	2	1	О-1,2 Д-1,2	С(1-2)	ОПК-3 ПК-20
2	Понятие защищенности в автоматизированных системах	2	1	О-1,3 Д-3-6	К(3-4)	ОПК-3 ПК-20
3	Основы законодательства РФ в области информационной безопасности и защиты информации	2	2	О-4,5 Д-3-6	К(5-6)	ОПК-3 ПК-20
4	Конфиденциальная информация и ее защита	2	3	О-1,2 Д-1,3-6	С(7-8)	ОПК-3 ПК-20
5	Лицензирование и сертификация в области обеспечения безопасности информации	2	4	О-2 Д-3,4	С(9-10)	ОПК-3 ПК-20
6	Технические средства обеспечения информационной безопасности	2	5	О-2,3, Д-3-5	С(11-12)	ОПК-3 ПК-20
7	Электромагнитные каналы утечки информации	2	6	О-1,3, Д-3,4	С(13-14)	ОПК-3 ПК-20
8	Электрические каналы утечки информации	2	7	О-1 Д-2,4,6	К(15-16)	ОПК-3 ПК-20
9	Угроза безопасности информации АСОД и субъектов информационных отношений	2	8	О-1,3, Д-3-6	К(17-18)	ОПК-3 ПК-20

К – контрольная работа, С – собеседование

4.2. Лабораторные работы и (или) практические занятия

4.2.1. Практические занятия

Таблица 4.3. – Практические занятия

№	Наименование практического занятия	Объем, час.
1	2	3
1	Практическая работа №1 «Алгоритм шифрования RSA»	2
2	Практическая работа №2 «Шифрование с помощью таблицы Виженера»	2
3	Практическая работа №3 «Скремблирование»	2
4	Практическая работа №4 «Алгоритм шифрования Эль – Гамаля»	2
5	Практическая работа №5 «Изучение демаскирующих признаков различных объектов»	2
6	Практическая работа №6 «Изучение существующих каналов утечки информации»	2
7	Практическая работа №7 «Количественная оценка стойкости	2

	парольной защиты»	
8	Практическая работа №8 «Реализация дискреционной модели политики безопасности»	2
Итого		18

4.2.2 Самостоятельная работа студентов (СРС)

Таблица 4.5 – 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	3,5
2.	Понятие защищенности в автоматизированных системах	3-4 недели	3,5
3.	Основы законодательства РФ в области информационной безопасности и защиты информации	5-6 недели	3,5
4.	Конфиденциальная информация и ее защита	7-8 недели	3,5
5.	Лицензирование и сертификация в области обеспечения безопасности информации	9-10 недели	3,5
6.	Технические средства обеспечения информационной безопасности	11-12 недели	3,5
7.	Электромагнитные каналы утечки информации	13-14 недели	3,5
8.	Электрические каналы утечки информации	15-16 недели	3,5
9.	Угроза безопасности информации АСОД и субъектов информационных отношений	17-19 недели	3,5
10.	Подготовка к экзамену	1-18 недели	4,4
Итого			35,9

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 требования ФГОС и Приказа Министерства образования и науки РФ от 5 апреля 2017г. №301 по специальности 38.05.01 «Экономическая безопасность» реализация компетентностного подхода предусматривает 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 33,3 процента от аудиторных занятий согласно УП.

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

№	Наименование раздела	Используемые интерактивные образовательные технологии	Объём, час.
1.	Практическая работа №1 «Алгоритм шифрования RSA» (практическое занятие)	Разбор конкретных ситуаций	6
2.	Комплексная защита информации и правовое регулирование информационной безопасности. .(лекция)	Разбор конкретных ситуаций	4
3.	Защита информации от случайных угроз. Дублирование информации. Повышение надежности компьютерных систем. (лекция)	Разбор конкретных ситуаций	4
4.	Основные законы в области защиты информации. Лицензирование в области защиты информации. (лекция)	Семинар	4

5.	Лабораторная работа 1 Изучение демаскирующих признаков различных объектов	Разбор конкретных ситуаций	6
	Итого		24

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
способность применять основные закономерности создания и принципы функционирования систем экономической безопасности хозяйствующих субъектов (ОПК-3)	Защита информации Информационная безопасность	Безопасность электронного документооборота Защита информационных процессов в компьютерных системах	Обеспечение экономической безопасности предприятий(организаций) Преддипломная практика Защита выпускной квалификационной работы, включая подготовку к процессу защиты и процедуру защиты
способность соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности (ПК-20)	Защита информации Информационная безопасность Практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-	Административное право Безопасность электронного документооборота Защита информационных процессов в компьютерных системах	Защита выпускной квалификационной работы, включая подготовку к процессу защиты и процедуру защиты

	исследовательской деятельности		

7.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Наименование компетенции	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно»)	Продвинутый уровень («хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
ОПК-3/ начальный	*1.Доля освоенных обучающимся знаний, умений навыков от общего объема ЗУН, установленных в п.1.ЗРПД* *2.Качество освоенных обучающимися 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-20/ начальный	*1.Доля освоенных обучающимся знаний, умений навыков от общего объема ЗУН, установленных в п.1.ЗРПД* *2.Качество освоенных обучающимися знаний, умений,*	Знать: - основные информационных и коммуникационных технологий Уметь: - находить необходимую информацию Владеть: - предоставления услуг по экономической	Знать: - основные принципы системы информационных и коммуникационных технологий Уметь: - анализировать полученную информацию Владеть: - навыками	Знать: - последние тенденции соответствующие требованиям потребителя Уметь: - предоставить готовый гостиничный продукт с помощью новейших технологий Владеть:

	навыков *3. Умение применять знания, умения, навыки в типовых и нестандартных ситуациях*	безопасности	освоения новейших информационных и коммуникационных технологий	- навыками разработки и предоставлению экономической безопасности

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 контролируемой компетенции (или её части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				Наименование	№ Заданий	
1	2	3	4	5	6	7
1	Введение в информационную безопасность	ОПК-3 ПК-20	Лекция, практические занятия №1, СРС	Тест Собеседование	1-10 МУ1: 1-30	В соответствии с таблицей 7.2
2	Понятие защищенности в автоматизированных системах	ОПК-3 ПК-20	Лекция, лабораторные №1 работы, СРС	Тест Собеседование	11-20 МУ5: 1-11	В соответствии с таблицей 7.2
3	Основы законодательства РФ в области информационной безопасности и защиты информации	ОПК-3 ПК-20	Лекция, практические занятия№2, СРС	Тест Собеседование	21-30 МУ2: 1-30	В соответствии с таблицей 7.2
4	Конфиденциальная информация и ее защита	ОПК-3 ПК-20	Лекция, лабораторные работы №2, СРС	Тест Собеседование	31-40 МУ6: 1-9	В соответствии с таблицей 7.2

5	Лицензирование и сертификация в области обеспечения безопасности информации	ОПК-3 ПК-20	Лекция, практические занятия №3, СРС	Тест Собеседование	41-50 МУ3: 1-30	В соответствии с таблицей 7.2
6	Технические средства обеспечения информационной безопасности	ОПК-3 ПК-20	Лекция, лабораторные работы №3 СРС	Тест Собеседование	51-60 МУ7: 1-12	В соответствии с таблицей 7.2
7	Электромагнитные каналы утечки информации	ОПК-3 ПК-20	Лекция, практические занятия №4, СРС	Тест Собеседование	61-70 МУ4: 1-30	В соответствии с таблицей 7.2
8	Электрические каналы утечки информации	ОПК-3 ПК-20	Лекция, лабораторные работы №4, СРС	Тест Собеседование	71-80 МУ8: 1-8	В соответствии с таблицей 7.2
9	Угроза безопасности информации АСОД и субъектов информационных отношений	ОПК-3 ПК-20	Лекция, СРС	Тест	81-100	В соответствии с таблицей 7.2

Примеры типовых контрольных заданий для текущего контроля

Примеры вопросов для собеседования

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.
8. Общая характеристика электромагнитного канала утечки информации
9. Сетевые атаки. Системы обнаружения атак
10. Виды конфиденциальной информации
11. Политика информационной безопасности
12. Определение информационной безопасности

Примеры тестовых заданий

1) Защита информации это:

1. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;

2. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;

3. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;

4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;

5. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

2) Информация это -

1.· сведения, поступающие от СМИ;

2.· только документированные сведения о лицах, предметах, фактах, событиях;

3. сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;

4.только сведения, содержащиеся в электронных базах данных.

3) Информация

1.· не исчезает при потреблении;

2. становится доступной, если она содержится на материальном носителе;

3. подвергается только "моральному износу";

4. характеризуется всеми перечисленными свойствами.

4) Что является объектом защиты информации?

1.вся информация в компьютере;

2.важная, для кого-либо информация;

3.информация, имеющая ценность для владельца компьютера;

4.информация, имеющая ценность для владельца и потенциального нарушителя компьютера.

5) Естественные угрозы безопасности информации вызваны:

1.деятельностью человека;

2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;

3. воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;

4. корыстными устремлениями злоумышленников;

5. ошибками при действиях персонала.

Типовые задания для промежуточной аттестации Промежуточная аттестация по дисциплине проводится в форме экзамена. Экзамен проводится в форме тестирования (бланкового и/или компьютерного).

Для тестирования используются контрольно-измерительные материалы (КИМ) – задания в тестовой форме, составляющие банк тестовых заданий (БТЗ) по дисциплине, утвержденный в установленном в университете порядке.

Проверяемыми на промежуточной аттестации элементами содержания являются темы дисциплины, указанные в разделе 4 настоящей программы. Все темы дисциплины отражены в КИМ в равных долях (%). БТЗ включает в себя не менее 100 заданий и постоянно пополняется.

Для проверки знаний используются вопросы и задания в различных формах:

-закрытой (с выбором одного или нескольких правильных ответов),

- открытой (необходимо вписать правильный ответ),

- на установление правильной последовательности,

- на установление соответствия.

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

В каждый вариант КИМ включаются задания по каждому проверяемому элементу содержания во всех перечисленных выше формах и разного уровня сложности. Такой формат КИМ позволяет объективно определить качество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

7.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

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

1	2	3	4	5
Практическая работа №1 «Алгоритм шифрования RSA»	1	Выполнил, но «не защитил»	3	Выполнил и «защитил»
Практическая работа №2 «Шифрование с помощью таблицы Виженера»	1	Выполнил, но «не защитил»	3	Выполнил и «защитил»
Практическая работа №3 «Скремблирование»	1	Выполнил, но «не защитил»	3	Выполнил и «защитил»
Практическая работа №4 «Алгоритм шифрования Эль – Гамаля»	1	Выполнил, но «не защитил»	3	Выполнил и «защитил»
Лабораторная работа №1 Изучение демаскирующих признаков различных объектов	2	Выполнил, но «не защитил»	3	Выполнил и «защитил»
Лабораторная работа №2 Изучение существующих каналов утечки информации	2	Выполнил, но «не защитил»	3	Выполнил и «защитил»
Лабораторная работа №3 Количественная оценка стойкости парольной защиты	2	Выполнил, но «не защитил»	3	Выполнил и «защитил»
Лабораторная работа №4 Реализация дискреционной модели политики безопасности	2	Выполнил, но «не защитил»	3	Выполнил и «защитил»
СРС	12		24	
Итого	24		48	
Посещаемость	0		16	
Экзамен	0		36	
Итого	24		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 2 балла,
- задание в открытой форме–2 балла,
- задание на установление правильной последовательности –2 балла,
- задание на установление соответствия –2 балла,
- решение задачи –6 баллов.

Максимальное количество баллов за тестирование - 36 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 защиты информации [Электронный ресурс] : учеб. пособие / Ю. Н. Загинайлов. – М . : Директ-Медиа, 2015. – 253с. - 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) Шифрование с помощью таблицы Виженера: методические указания к выполнению практических работ по дисциплинам: «Защита информации», «Информационная безопасность» / Юго-Зап. гос. ун-т; сост. А.Л. Марухленко. Курск, 2017.

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

4) 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.

5) Изучение демаскирующих признаков различных объектов: методические указания к выполнению лабораторных работ по дисциплинам: «Защита информации», «Информационная безопасность» / Юго-Зап. гос. ун-т; сост. А.Л. Марухленко. Курск, 2017.

6) Изучение существующих каналов утечки информации: методические указания к выполнению лабораторных работ по дисциплинам: «Защита информации», «Информационная безопасность» / Юго-Зап. гос. ун-т; сост. А.Л. Марухленко. Курск, 2017.

7) Количественная оценка стойкости парольной защиты: методические указания к выполнению лабораторных работ по дисциплинам: «Защита информации», «Информационная безопасность» / Юго-Зап. гос. ун-т; сост. А.Л. Марухленко. Курск, 2017.

8) Реализация дискреционной модели политики безопасности: методические указания к выполнению лабораторных работ по дисциплинам: «Защита информации», «Информационная безопасность» / Юго-Зап. гос. ун-т; сост. А.Л. Марухленко. Курск, 2017.

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)
- VMware workstation

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: ноутбук ASUSX50VLPMD-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			