Аннотация к рабочей программе дисциплины «Информационная безопасность»

Цель преподавания дисциплины.

Формирование знаний по информационной безопасности (ИБ), необходимых специалистам для проектирования, внедрения и эксплуатации корпоративных вычислительных и информационных систем (ВС/ИС).

Задачи изучения дисциплины.

Освоение технологий диагностики опасностей и угроз для информационных систем и методов работы с моделями безопасности. Разбираются основные типы угроз и способы парирования таких угроз: каналы утечки информации, компьютерные вирусы, закладки, атаки на информационные системы, имеющие доступ к глобальным телекоммуникациям (несанкционированный доступ с применением сетевых технологий).

Компетенции, формируемые в результате освоения дисциплины:

− 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).

Разделы дисциплины.

Создание всеобщего информационного пространства; основные понятия «защита информации», «информационная безопасность», «угроза информационной безопасности». Доктрина информационной безопасности Российской Федерации. Национальные интересы Российской Федерации в информационной сфере и их обеспечение. Состояние информационной безопасности Российской Федерации и основные задачи по ее обеспечению. Концепции корпоративных информационных систем. Подходы к разработке корпоративных систем. Информация, являющаяся государственной, коммерческой или персональной тайной. Классификация защищаемой информации. Защищенные информационные технологии в Internet. Защита архитектуры «клиент – сервер». Анализ защищенности операционных систем. Защита каналов связи в Internet. Отечественные защищенные системы. Интегральные устройства защиты информации. Программа информационной безопасности организации. Стандарты безопасности Гостехкомиссии. Стандарты Европы и США. Международная электротехническая комиссия. Классы информационной безопасности. Модель выбора варианта инфраструктуры защиты информации бизнес-процессов. Критерии эффективности средств защиты информации.

МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

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

Т.Ю. Ткачева
(подпись, инициалы, фамилия)
«01» марта 2017 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 – 2017

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 2017 г. на заседании кафедры ИБ, протокол №12 от 29.06.18г.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой Таныгин М.О.

Рабочая программа переесмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана специальности 38.05.01 «Экономическая безопасность», одобренного Ученым советом университета протокол №9 «26» 03 2018 г. на заседании кафедры информационной безопасности, протокол №1 от 31.08.2018

(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 №9 «21» 02 2019 г. на заседании кафедры информационной безопасности, протокол №1 от 31.08.2020

(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 №7 «25» 02 2020 г. на заседании кафедры информационной безопасности, протокол №1 от 30.08.21

(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 №_ «__»_____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

1. Ознакомление с принципами, базовыми определениями и вариантами организации защиты информации;
2. Ознакомление с актуальной нормативно-правовой базой РФ по части информационной безопасности.
3. Изучение угроз информационной безопасности, моделей поведения злоумышленника, основ работы с конфиденциальными данными;
4. Ознакомление с основами защиты авторских прав, работы с персональными данными;
5. Изучения способов выявления контрафактной продукции;
6. Изучение, в том числе на практическом уровне, основ криптографических преобразований в части потоковых шифров, ассиметричных систем и перспективных методов защиты.
7. Ознакомление с технологиями защиты программного обеспечения.

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

– возможные каналы утечки конфиденциальной информации;

– нормативно-правовые аспекты обеспечения информационной безопасности РФ;

– классификацию криптографических методов

– основы шифрования с помощью скремблеров, ассиметричных алгоритмов, перспективными методами.

уметь:

– принимать управленческие решения для решения профессиональных задач

– снижать вероятность отрицательных последствий сетевого взаимодействия;

– классифицировать угрозы информационной безопасности;

– выполнять шифрование криптографическими методами;

– определять целесообразность применения тех или иных методов защиты;

– анализировать статистику распределения данных после шифрования.

владеть:

– навыками быстрого поиска и анализа полученной информации

– навыками шифрования в режиме ручного расчета;

– 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.02 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 единицы, 72 академических часа.

Таблица 3.1 – Объём дисциплины по видам учебных занятий

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	72
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	36
в том числе:	
лекции	18
лабораторные занятия	18
практические занятия	0
Самостоятельная работа обучающихся (всего)	35,9
Контроль (подготовка к экзамену)	0
Контактная работа по промежуточной аттестации (всего АттКР)	0,1
в том числе:	
зачет	0,1
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрена
экзамен (включая консультацию перед экзаменом)	не предусмотрен

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.	Базовые понятия	Термины и определения. Информация как предмет защиты. Субъекты информационных отношений. Организация системы защиты информации. Комплексная защита информационных систем
2.	Конфиденциальность. Классификация угроз	Работа с конфиденциальными данными. Угрозы информационной безопасности. Модель поведения нарушителя. Классификация угроз
3.	Угрозы ИБ. Классы нарушителей. Оценка риска	Угрозы утечки по техническим каналам, уязвимости каналов взаимодействия. Анализ сетевого трафика. Сканирование сети. Угрозы выявления пароля. Подмена доверенного объекта. Навязывание ложного маршрута. Внедрение ложного объекта. Отказ в обслуживании. Распространение вредоносных программ и удаленный запуск. Оценка угроз по классам нарушителей. Субъективная оценка вероятности реализации угроз

4.	Персональные данные. Защита авторских прав	Обработка персональных данных. Защита интеллектуальной собственности. Авторское право. Гражданско-правовая ответственность. Административная ответственность. Уголовная ответственность
5.	Выявление контрафактной продукции	**Выявление контрафактной продукции.** Выбор оптимальных методов контроля и защиты информационной систем. Лицензирование программных продуктов. Интеграция механизмов защиты в программное обеспечение для борьбы с НСД.
6.	Криптографические методы защиты	Основы криптографии, методы защиты. Классификация криптографических методов. Потоковые шифры. Скремблирование. Ассиметричные шифры. Клеточные автоматы

Таблица 4.2 – Содержание дисциплины и ее методическое обеспечение

№ Пп/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.	Базовые понятия	4			У-1-5 МО 1-3	С,Т (1-2)	ОПК-3 ПК-20
2.	Конфиденциальность. Классификация угроз	4			У-1-4 МО 1-6	С,Т (2-4)	ОПК-3 ПК-20
3.	Угрозы ИБ. Классы нарушителей. Оценка риска	4		1	У-3-5 МО 3-6	С, Т (4-6)	ОПК-3 ПК-20
4.	Персональные данные. Защита авторских прав	4		6	У-1	С, Т (6-8)	ОПК-3 ПК-20
5.	Выявление контрафактной продукции	4			У-1	С, Т (9-13)	ОПК-3 ПК-20
6.	Криптографические методы защиты	16		2-5	У-1 МО 4,5	С ,Т (6-18)	ОПК-3 ПК-20
	Всего	36	0				

С – собеседование, Т – тестирование

4.2 Лабораторные работы и (или) практические занятия

4.2.1. Практические занятия

Таблица 4.3. – Практические занятия

№	Наименование	Объем, час.
1.	Анализ защищенности вычислительной системы	2
2.	Шифры полиалфавитной замены	2
3.	Потоковые шифры. Скремблирование бинарного потока данных	4
4.	Ассиметричные клиптоалгоритмы. Метод RSA	4
5.	Обработка на базе клеточных автоматов	4
6.	Интеграция механизмов защиты в программное обеспечение	2
Итого		18

4.2.2 Самостоятельная работа студентов (СРС)

Таблица 4.5 – Самостоятельная работа студентов

№	Наименование раздела учебной дисциплины	Срок выполнения, недели	Время, затрачиваемое на выполнение СРС, час.
1.	Базовые понятия	1-2	2
2.	Конфиденциальность. Классификация угроз	2-3	4
3.	Угрозы ИБ. Классы нарушителей. Оценка риска	3-8	4
4.	Персональные данные. Защита авторских прав	7-9	5.9
5.	Выявление контрафактной продукции	9-12	3
6.	Криптографические методы защиты	4-18	15
7.	Подготовка реферата на заданную тему	4-18	2
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 или зачету, 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. Технологии использования воспитательного потенциала дисциплины

В соответствии с требованиями ФГОС и приказа Минобрнауки России № 301 от 05.04.2017 г. по направлению подготовки 38.05.01 «Экономическая безопасность» 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 30 процентов от аудиторных занятий согласно УП.

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

№	Наименование раздела	Используемые интерактивные образовательные технологии	Объём, час.
лекции			
1.	Криптографические методы защиты. Замена, потоковые шифры, блочные шифры, перспективные методы защиты.	Разбор конкретных ситуаций, семинар	6
практика			
2.	Выполнение работы «Потоковые шифры. Скремблирование бинарного потока данных»	Разбор конкретных ситуаций, семинар	2
3.	Выполнение работы «Ассиметричные клиптоалгоритмы. Метод RSA»	Разбор конкретных ситуаций, семинар	2
4.	Выполнение работы «Обработка на базе клеточных автоматов»	Разбор конкретных ситуаций, семинар	2
	Итого		12

Содержание дисциплины обладает значительным воспитательным потенциалом, поскольку в нем аккумулирован научный опыт человечества. Реализация воспитательного потенциала дисциплины осуществляется в рамках единого образовательного и воспитательного процесса и способствует непрерывному развитию личности каждого обучающегося. Дисциплина вносит значимый вклад в формирование общей и профессиональной культуры обучающихся. Содержание дисциплины способствует правовому, экономическому, профессионально-трудовому, воспитанию обучающихся.

Реализация воспитательного потенциала дисциплины подразумевает:

– целенаправленный отбор преподавателем и включение в лекционный материал, материал для практических и (или) лабораторных занятий содержания, демонстрирующего обучающимся образцы настоящего научного подвижничества создателей и представителей данной отрасли науки (производства, экономики, культуры), высокого профессионализма ученых (представителей производства, деятелей культуры), их ответственности за результаты и последствия деятельности для человека и общества; примеры подлинной нравственности людей, причастных к развитию науки и производства;

– применение технологий, форм и методов преподавания дисциплины, имеющих высокий воспитательный эффект за счет создания условий для взаимодействия обучающихся с преподавателем, другими обучающимися, (командная работа, разбор конкретных ситуаций)*;*

– личный пример преподавателя, демонстрацию им в образовательной деятельности и общении с обучающимися за рамками образовательного процесса высокой общей и профессиональной культуры.

Реализация воспитательного потенциала дисциплины на учебных занятиях направлена на поддержание в университете единой развивающей образовательной и воспитательной среды. Реализация воспитательного потенциала дисциплины в ходе самостоятельной работы обучающихся способствует развитию в них целеустремленности, инициативности, креативности, ответственности за результаты своей работы – качеств, необходимых для успешной социализации и профессионального становления.

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)	Бухгалтерский учет	Бухгалтерский учет Информационная безопасность	Обеспечение экономической безопасности предприятий(организаций) Преддипломная практика
способность соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности (ПК-20)	Практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности	Административное право Информационная безопасность	

7.2. Описание показателей и критериев оценивания компетенций на раз- личных 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/ начальый, основной, звершающий	*1.Доля освоенных обучающимся знаний, умений навыков от общего объема ЗУН, установленных в п.1.ЗРПД 2.Качество освоенных*	Знать: - основные принципы законы физические явления и процессы Уметь: -анализировать Владеть: - навыками применения	Знать: - основные принципы системы информационной безопасности Уметь: - отыскать необходимую информацию Владеть:	Знать: - основные принципы системы информационной безопасности и защиты информации Уметь: - принимать управленческие

	обучающимися знаний, умений, навыков *3. Умение применять знания, умения, навыки в типовых и нестандартных ситуациях*	законов в конкретной жизненной ситуации	- навыками анализировать полученную информацию	решения для решения профессиональных задач Владеть: - навыками быстрого поиска и анализа полученной информации
ПК-20/начальный, основной	*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 информационных и коммуникационных технологий – классификацию криптографических методов – основы шифрования с помощью скремблеров, ассиметричных алгоритмов, перспективными методами. Уметь: - находить необходимую информацию Владеть: - предоставления услуг по экономической безопасности	Знать: - основные принципы системы информационных технологий Уметь: - анализировать полученную информацию –выполнять шифрование криптографическими методами; –определять целесообразность применения методов защиты; –анализировать статистику распределения данных после шифрования. Владеть: - навыками освоения актуальных технологий	Знать: - последние тенденции, соответствующие требованиям потребителя Уметь: - предоставить готовый гостиничный продукт с помощью новейших технологий Владеть: - навыками разработки и предоставлению экономической безопасности - навыками шифрования в режиме ручного расчета;

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 компе-тенции (или её части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наим	№№ заданий	
1	2	3	4	5	6	7
1.	Базовые понятия	УК-1 ОПК-1	Лекция, СРС	Собеседование,	1-5	Согласно табл.7.2
				Тестирование	1-25	
2.	Конфиденциальность. Классификация угроз	УК-1 ОПК-1	Лекция, СРС	Собеседование,	1-5	Согласно табл.7.2
				Тестирование	1-24	
3.	Угрозы ИБ. Классы нарушителей. Оценка риска	УК-1 ОПК-1	Лекция, СРС	Собеседование,	1-5	Согласно табл.7.2
				Тестирование	1-5	
4.	Персональные данные. Защита авторских прав	ОПК-1	Лекция, СРС	Собеседование,	1-5	Согласно табл.7.2
				Тестирование	1-5	
5.	Выявление контрафактной продукции	ОПК-9	Лекция, СРС, практические работы	Собеседование,	1-5	Согласно табл.7.2
				Тестирование	1-5	
6.	Криптографические методы защиты	ОПК-1	Лекция, СРС	Собеседование, Тестирование	1-42	Согласно табл.7.2

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы в тестовой форме по теме 1. «Базовые понятия.»

1) Защита информации это:

А) процесс сбора, накопления, обработки, хранения, распределения и поиска информации;

Б) преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;

В) получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;

Г) совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;

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

Темы рефератов

1) Современные средства видеонаблюдения
2) Методы контроля целостности информации
3) Защиты программ от изучения и отладки
4) Методы защиты от действий хакеров
5) Обзор совершенных компьютерных преступлений

6) Методы ограничения доступа к ресурсам вычислительной сети
7) Протоколы SSL и TLS
8) Системы идентификации по индивидуальным характеристикам человека
9) Организация защищенного документооборота. Виртуальные частные сети
10) Технические каналы утечки акустической информации
11) Защита телефонных разговоров
12) Сертификация средств защиты информации
13) Законодательные основы в области защиты персональных данных
14) Противодействие утечке информации
15) Защита информации в Интернет
16) Технология защиты вычислительной системы от вирусов
17) Криптографические хеш-функции
18) Защита программ от несанкционированного запуска
19) Принципы и методы защиты оптических дисков
20) Парольная защита. Программы-шпионы
21) Криптографические алгоритмы с открытым ключом и их использование
22) Поточные шифры и генераторы псевдослучайных чисел.
23) Простейшие методы шифрования с закрытым ключом
24) Основы защиты авторских прав
25) Электронные деньги.
26) Классификация угроз и объектов защиты
27) Системы контроля доступа и учета рабочего времени
28) Аппаратное шифрование.
29) Социальные методы взлома
30) Защита информации в музыке
31) Защита информации от утечки по техническим каналам
32) Обзор корпоративных межсетевых экранов
33) Обзор алгоритмов ЭЦП
34) Технология BlockChain.
35) Обзор систем обнаружения утечек информации (DLP)
36) Обзор средств защиты в системах интернет-банкинга
37) Лицензирование в области защиты информации: лицензии ФСБ и ФСТЭК
38) Защита персональных данных: закон, подзаконные акты, основные понятия и положения, организационные и технические требования
39) Основные методики оценки рисков информационной безопасности
40) Обзор средств защиты от НСД, имеющих сертификат ФСТЭК
41) Хранение, обработка и уничтожение конфиденциальных документов

42) Обзор стандартов защиты информации: серия стандартов СТО БР ИББС

43) Система сертификации средств защиты информации по требованиям безопасности информации: стандарты, виды и порядок сертификации

44) История развития вирусов и антивирусов, различные виды вирусов.

45) Основные принципы обеспечения информационной безопасности

46) Понятие защищенности автоматизированных систем

47) Меры и средства защиты информации

48) Основы законодательства РФ в области информационной безопасности и защиты информации

49) Лицензирование и сертификация в области обеспечения безопасности информации

50) Международное право в сфере защиты информации

51) Организационное обеспечение информационной безопасности

52) Электромагнитные каналы утечки информации

53) Электрические каналы утечки информации

54) Способы и средства подавления электронных устройств перехвата речевой информации

55) Угрозы безопасности информации, АСОД и субъектов информационных отношений

56) Основные подходы к проектированию систем защиты информации

57) Идентификация, аутентификация и разграничение доступа

58) Методы обнаружения и удаления компьютерных вирусов

59) Симметричные и ассиметричные криптографические системы

60) Классификация угроз безопасности операционных систем

61) Управление целостностью данных

62) Методы воздействий нарушителя на корпоративную сеть

63) Межсетевые экраны

64) Системы обнаружения атак

65) Виртуальные частные сети

66) Информационная безопасность геоинформационных систем

67) Современные средства защиты информации от НСД

Примеры вопросов для собеседования

1. Определение информации.
2. Компьютерные вирусы, их классификация.
3. Виды угроз информации.
4. Алгоритмы шифрования.
5. Криптостойкость.
6. Аутентификация и авторизация.

7. Общая характеристика электромагнитного канала утечки информации
8. Сетевые атаки. Системы обнаружения атак
9. Виды конфиденциальной информации
10. Политика информационной безопасности
11. Основы безопасной работы в Интернет
12. Почему при шифровании методом RSA размер блока увеличивается?

Вопросы для защиты практических работ приведены в соответствующих разделах п.4 основной литературы (У-1).

Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине проводится в форме зачета. Зачет 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.

Примеры типовых заданий для проведения промежуточной аттестации обучающихся:

Задание в закрытой форме:

..... 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.

Задание в открытой форме:

..... Выделяют три основные компоненты информационной системы (указать какие?):

1)……2)…….……3)…….

Задание на установление правильной последовательности,

..... Содержание технологического процесса обработки информации включает ряд процедур. Укажите их правильную последовательность:

- обработка информации;
- хранение;
- сбор;
- визуализация.

Задание на установление соответствия:

Какая технология используется для получения данных из Интернета:

1. файл-сервер; 2. клиент-сервер; 3. Интернет-технология; 4. удаленная технология.

Компетентностно-ориентированная задача:

Приведите процедуру аутентификации пользователя со следующими исходными данными: имя пользователя (Name), пароль (Password), случайное число (V). Процедура перемешивания состоит в последовательном перемешивании полубайтов пароля и случайного числа. Вычисление дайджеста состоит в вычислении остатка перемешенного числа по модулю Password.

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 «О балльно-рейтинговой системе оценивания результатов обучения по дисциплинам (модулям) и практикам при освоении обучающимися 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
Выполнение работы №1 Анализ защищенности вычислительной системы	2	Выполнил, но «не защитил»	2	Выполнил и «защитил»
Выполнение работы №2 Шифры полиалфавитной замены	2	Выполнил, но «не защитил»	3	Выполнил и «защитил»
Выполнение работы №3 Потоковые шифры. Скремблирование бинарного потока данных	2	Выполнил, но «не защитил»	5	Выполнил и «защитил»
Выполнение работы №4 Ассиметричные клиптоалгоритмы. Метод RSA	2	Выполнил, но «не защитил»	8	Выполнил и «защитил»
Выполнение работы №5 Обработка на базе перспективных методов	10	Выполнил, но «не защитил»	10	Выполнил и «защитил»
Выполнение работы №6 Интеграция механизмов защиты в программное обеспечение	4	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Реферат на заданную тему	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
СРС	0		12	
ИТОГО	24		48	
Посещаемость	0		16	
Зачет	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 компетентностно-ориентированной задачи –6 баллов.

Максимальное количество баллов за тестирование - 36 баллов.

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

8.1 Основная литература

1) Технологии обеспечения безопасности информационных систем : учебное пособие : [16+] / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов и др. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с. : ил., схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=598988 (дата обращения: 07.09.2021). – Библиогр.: с. 196-205. – ISBN 978-5-4499-1671-6. – DOI 10.23681/598988. – Текст : электронный.

2) Ищейнов, Вячеслав Яковлевич. Защита конфиденциальной информации [Текст] : учебное пособие / В. Я. Ищейнов, М. В. Мецатунян. - Москва : Форум, 2013. - 256 с.

8.2 Дополнительная литература

3) Организационно-правовое обеспечение информационной безопасности [Текст] : учебное пособие / под ред. А. А. Стрельцова. - М. : Академия, 2008. - 256 с.

4) Романов, О. А. Организационное обеспечение информационной безопасности [Текст] : учебник / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М. : Академия, 2008. - 192 с.

5) Спицын, В. Г. Информационная безопасность вычислительной техники : учебное пособие / В. Г. Спицын ; Томский Государственный университет систем управления и радиоэлектроники (ТУСУР). – Томск : Эль Контент, 2011. – 148 с. – URL: https://biblioclub.ru/index.php?page=book&id=208694 (дата обращения: 27.08.2021). – Режим доступа: по подписке. – Текст : электронный.

8.3 Перечень методических указаний

1) Виды информации и основные методы ее защиты : методические указания по выполнению работы по дисциплине / Юго-Зап. гос. ун-т ; сост. А. Л. Марухленко. - Курск : ЮЗГУ, 2017. - 8 с. - Текст : электронный.

2) Виды угроз информационной безопасности Российской Федерации : методические указания / Юго-Зап. гос. ун-т ; сост. А. Л. Марухленко. - Курск : ЮЗГУ, 2017. - 7 с. - Текст : электронный.

3) Источники угроз информационной безопасности Российской Федерации : методические указания / Юго-Зап. гос. ун-т ; сост. А. Л. Марухленко. - Курск : ЮЗГУ, 2017. - 8 с. - Текст : электронный.

4) Защита от утечек по каналу ПЭМИН, по акустическому и виброакустическому каналам : методические указания по выполнению лабораторной работы по дисциплине / Юго-Зап. гос. ун-т ; сост. А. Л. Марухленко. - Курск : ЮЗГУ, 2017. - 7 с. - Текст : электронный.

5) Анализ трафика и сбор критичной информации программами пассивного анализа : методические указания по выполнению лабораторной работы по дисциплине «Основы информационной безопасности» / Юго-Зап. гос. ун-т ; сост. А. Л. Марухленко. - Курск : ЮЗГУ, 2017. - 6 с. - Текст : электронный.

6) Аудит комплексной защиты информации предприятия : методические указания по выполнению лабораторной работы по дисциплине «Основы информационной безопасности» / Юго-Зап. гос. ун-т ; сост. А. Л. Марухленко. - Курск : ЮЗГУ, 2017. - 8 с. - Текст : электронный.

8. 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)

9. Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Информационная безопасность» являются лекции и практические 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 практические 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.

Практическому 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 практическим работам, а также по результатам докладов.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины: 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 практическим 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”.

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

Microsoft Office 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №K0000000117 от 21.12.2015 г. с ООО «СМСКанал», Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234,Windows, договор IT000012385, Oracle Virtualbox (Бесплатная, GNU General Public License), редактор двоичных файлов Free Hex Editor Neo, (Свободное ПО http://www.hhdsoftware.com/free-hex-editor), портал верификации результатов выполнения практических заданий (https://x46.herokuapp.com) (свободное ПО).

11. 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 на базе CPU AMD-Phenom, ОЗУ 8 GB, HDD 1 Tb, монитор Aok 21” и выше. Проекционный экран на штативе; Мультимедиацентр: ноутбук ASUSX50VLPMD-T2330/14"/1024Mb/160Gb, проектор inFocusIN24+.

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

Компьютерные классы кафедры информационные системы и технологии, оснащены учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска.

Мультимедиа центр: ноутбук ASUSX50VL PMD-T2330/1471024Mb/1 60Gb/

Проектор inFocusIN24+ (39945,45)– 1 шт.

Многофункциональное устройство Canon MF4018 -1 шт.

Многофункциональное устройство Brother MFC-7420R- 3 шт.

Многофункциональное устройство Brother DCP-8065DN- 1 шт.

Принтер 3D UP - 1 шт.

Компьютерный класс а-214.

Компьютер ВАРИАНТ PDC2160/iC33/2*512Mb/ HDD160Gb/DVD-ROM/FDD/ATX350W/K/m/WXP/0 FF/17"TFTE700 (18809.20) – 10 шт;

Вычислительный комплекс имитационного моделирования – 3 шт;

Компьютерный класс а-207

Компьютер IntelCore i3-4330, 3.5GHz, 8Gb, 500Gb HDD, LCD Philips 21”– 10 шт;

13 Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.). Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).

14 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			

МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

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

Т.Ю. Ткачева
(подпись, инициалы, фамилия)
«01» марта 2017 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 *заочная*
очная, очно-заочная, заочная

Курск – 2017

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 2017 г. на заседании кафедры ИБ, протокол №12 от 29.06.18г.

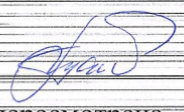
(наименование кафедры, дата, номер протокола)

Зав. кафедрой Таныгин М.О.

Рабочая программа переесмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана специальности 38.05.01 «Экономическая безопасность», одобренного Ученым советом университета протокол №9 «26» 03 2018 г. на заседании кафедры информационной безопасности, протокол №1 от 31.08.2018

(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 №9 «21» 02 2019 г. на заседании кафедры информационной безопасности, протокол №1 от 31.08.2020

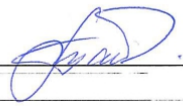
(наименование кафедры, дата, номер протокола)

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 №7 «25» 02 2020 г. на заседании кафедры информационной безопасности, протокол №1 от 30.08.21

(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 №_ «__»_____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

1. Ознакомление с принципами, базовыми определениями и вариантами организации защиты информации;
2. Ознакомление с актуальной нормативно-правовой базой РФ по части информационной безопасности.
3. Изучение угроз информационной безопасности, моделей поведения злоумышленника, основ работы с конфиденциальными данными;
4. Ознакомление с основами защиты авторских прав, работы с персональными данными;
5. Изучения способов выявления контрафактной продукции;
6. Изучение, в том числе на практическом уровне, основ криптографических преобразований в части потоковых шифров, ассиметричных систем и перспективных методов защиты.
7. Ознакомление с технологиями защиты программного обеспечения.

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

– возможные каналы утечки конфиденциальной информации;

– нормативно-правовые аспекты обеспечения информационной безопасности РФ;

– классификацию криптографических методов

– основы шифрования с помощью скремблеров, ассиметричных алгоритмов, перспективными методами.

уметь:

– принимать управленческие решения для решения профессиональных задач

– снижать вероятность отрицательных последствий сетевого взаимодействия;

– классифицировать угрозы информационной безопасности;

– выполнять шифрование криптографическими методами;

– определять целесообразность применения тех или иных методов защиты;

– анализировать статистику распределения данных после шифрования.

владеть:

– навыками быстрого поиска и анализа полученной информации

– навыками шифрования в режиме ручного расчета;

– 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.02 вариативной части базового цикла учебного плана по специальности 38.05.01 «Экономическая безопасность», заочная форма обучения, изучаемую в 4, 5 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 единицы, 72 академических часа.

Таблица 3.1 – Объём дисциплины по видам учебных занятий

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	72
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	8
в том числе:	
лекции	4
лабораторные занятия	4
практические занятия	0
Самостоятельная работа обучающихся (всего)	59,9
Контроль (подготовка к экзамену)	0
Контактная работа по промежуточной аттестации (всего АттКР)	0,1
в том числе:	
зачет	0,1
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрена
экзамен (включая консультацию перед экзаменом)	не предусмотрен

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.	Базовые понятия	Термины и определения. Информация как предмет защиты. Субъекты информационных отношений. Организация системы защиты информации. Комплексная защита информационных систем
2.	Конфиденциальность. Классификация угроз	Работа с конфиденциальными данными. Угрозы информационной безопасности. Модель поведения нарушителя. Классификация угроз
3.	Угрозы ИБ. Классы нарушителей. Оценка риска	Угрозы утечки по техническим каналам, уязвимости каналов взаимодействия. Анализ сетевого трафика. Сканирование сети. Угрозы выявления пароля. Подмена доверенного объекта. Навязывание ложного маршрута. Внедрение ложного объекта. Отказ в обслуживании. Распространение вредоносных программ и удаленный запуск. Оценка угроз по классам нарушителей. Субъективная оценка

		вероятности реализации угроз
4.	Персональные данные. Защита авторских прав	Обработка персональных данных. Защита интеллектуальной собственности. Авторское право. Гражданско-правовая ответственность. Административная ответственность. Уголовная ответственность
5.	Выявление контрафактной продукции	**Выявление контрафактной продукции.** Выбор оптимальных методов контроля и защиты информационной систем. Лицензирование программных продуктов. Интеграция механизмов защиты в программное обеспечение для борьбы с НСД.
6.	Криптографические методы защиты	Основы криптографии, методы защиты. Классификация криптографических методов. Потоковые шифры. Скремблирование. Ассиметричные шифры. Клеточные автоматы

Таблица 4.2 – Содержание дисциплины и ее методическое обеспечение

№ Пп /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.	Базовые понятия	4			У-1-5 МО 1-3	С,Т (1-2)	ОПК-3 ПК-20
2.	Конфиденциальность. Классификация угроз				У-1-4 МО 1-6	С,Т (2-4)	ОПК-3 ПК-20
3.	Угрозы ИБ. Классы нарушителей. Оценка риска			1	У-3-5 МО 3-6	С, Т (4-6)	ОПК-3 ПК-20
4.	Персональные данные. Защита авторских прав			6	У-1	С, Т (6-8)	ОПК-3 ПК-20
5.	Выявление контрафактной продукции				У-1	С, Т (9-13)	ОПК-3 ПК-20
6.	Криптографические методы защиты			2-5	У-1 МО 4,5	С ,Т (6-18)	ОПК-3 ПК-20
	Всего	4	0				

С – собеседование, Т – тестирование

4.2. Лабораторные работы и (или) практические занятия

4.2.1. Практические занятия

Таблица 4.3. – Практические занятия

№	Наименование	Объем, час.
1.	Анализ защищенности вычислительной системы	1
2.	Шифры полиалфавитной замены	1
3.	Потоковые шифры	2
Итого		4

4.2.2 Самостоятельная работа студентов (СРС)

Таблица 4.5 – Самостоятельная работа студентов

№	Наименование раздела учебной дисциплины	Срок выполнения, недели	Время, затрачиваемое на выполнение СРС, час.
1.	Базовые понятия	1-2	5
2.	Конфиденциальность. Классификация угроз	2-3	6
3.	Угрозы ИБ. Классы нарушителей. Оценка риска	3-8	6
4.	Персональные данные. Защита авторских прав	7-9	5.9
5.	Выявление контрафактной продукции	9-12	8
6.	Криптографические методы защиты	4-18	25
7.	Подготовка реферата на заданную тему	4-18	4
Итого			59,9

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 или зачету, 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. Технологии использования воспитательного потенциала дисциплины

В соответствии с требованиями ФГОС и приказа Минобрнауки России № 301 от 05.04.2017 г. по направлению подготовки 38.05.01 «Экономическая безопасность» 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 30 процентов 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.	Криптографические методы защиты. Замена, потоковые шифры	Разбор конкретных ситуаций, семинар	2

Содержание дисциплины обладает значительным воспитательным потенциалом, поскольку в нем аккумулирован научный опыт человечества. Реализация воспитательного потенциала дисциплины осуществляется в рамках единого образовательного и воспитательного процесса и способствует непрерывному развитию личности каждого обучающегося. Дисциплина вносит значимый вклад в формирование общей и профессиональной культуры обучающихся. Содержание дисциплины способствует правовому, экономическому, профессионально-трудовому, воспитанию обучающихся.

Реализация воспитательного потенциала дисциплины подразумевает:

– целенаправленный отбор преподавателем и включение в лекционный материал, материал для практических и (или) лабораторных занятий содержания, демонстрирующего обучающимся образцы настоящего научного подвижничества создателей и представителей данной отрасли науки (производства, экономики, культуры), высокого профессионализма ученых (представителей производства, деятелей культуры), их ответственности за результаты и последствия деятельности для человека и общества; примеры подлинной нравственности людей, причастных к развитию науки и производства;

– применение технологий, форм и методов преподавания дисциплины, имеющих высокий воспитательный эффект за счет создания условий для взаимодействия обучающихся с преподавателем, другими обучающимися, (командная работа, разбор конкретных ситуаций)*;*

– личный пример преподавателя, демонстрацию им в образовательной деятельности и общении с обучающимися за рамками образовательного процесса высокой общей и профессиональной культуры.

Реализация воспитательного потенциала дисциплины на учебных занятиях направлена на поддержание в университете единой развивающей образовательной и воспитательной среды. Реализация воспитательного потенциала дисциплины в ходе самостоятельной работы обучающихся способствует развитию в них целеустремленности, инициативности, креативности, ответственности за результаты своей работы – качеств, необходимых для успешной социализации и профессионального становления.

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)	Бухгалтерский учет	Бухгалтерский учет Информационная безопасность	Обеспечение экономической безопасности предприятий(организаций) Преддипломная практика

способность соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности (ПК-20)	Практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности	Административное право Информационная безопасность	

7.2. Описание показателей и критериев оценивания компетенций на раз- личных 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, основной, завершающий	*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/на	*1.Доля освоенных*	Знать: - основные	Знать: - основные	Знать: - последние

чальный, основной	*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*	информационных и коммуникационных технологий – классификацию криптографических методов – основы шифрования с помощью скремблеров, ассиметричных алгоритмов, перспективными методами. Уметь: - находить необходимую информацию Владеть: - предоставления услуг по экономической безопасности	принципы системы информационных технологий Уметь: - анализировать полученную информацию –выполнять шифрование криптографическими методами; –определять целесообразность применения методов защиты; –анализировать статистику распределения данных после шифрования. Владеть: - навыками освоения актуальных технологий	тенденции, соответствующие требованиям потребителя Уметь: - предоставить готовый гостиничный продукт с помощью новейших технологий Владеть: - навыками разработки и предоставлению экономической безопасности - навыками шифрования в режиме ручного расчета;

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 компе-тенции (или её части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наим	№№ заданий	
1	2	3	4	5	6	7
1.	Базовые понятия	УК-1 ОПК-1	Лекция, СРС	Собеседование,	1-5	Согласно табл.7.2
				Тест	1-25	
2.	Конфиденциальность. Классификация угроз	УК-1 ОПК-1	Лекция, СРС	Собеседование,	1-5	Согласно табл.7.2
				Тест	1-24	
3.	Угрозы ИБ. Классы нарушителей. Оценка	УК-1 ОПК-1	Лекция, СРС	Собеседование,	1-5	Согласно табл.7.2

	риска			Тест	1-5	
4.	Персональные данные. Защита авторских прав	ОПК-1	Лекция, СРС	Собеседование,	1-5	Согласно табл.7.2
				Тест	1-5	
5.	Выявление контрафактной продукции	ОПК-9	Лекция, СРС, практические работы	Собеседование,	1-5	Согласно табл.7.2
				Тест	1-5	
6.	Криптографические методы защиты	ОПК-1	Лекция, СРС	Собеседование, тест	1-42	Согласно табл.7.2

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы в тестовой форме по теме 1. «Базовые понятия.»

1) Защита информации это:

А) процесс сбора, накопления, обработки, хранения, распределения и поиска информации;

Б) преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;

В) получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;

Г) совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;

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

Темы рефератов

1) Современные средства видеонаблюдения
2) Методы контроля целостности информации
3) Защиты программ от изучения и отладки
4) Методы защиты от действий хакеров
5) Обзор совершенных компьютерных преступлений
6) Методы ограничения доступа к ресурсам вычислительной сети
7) Протоколы SSL и TLS
8) Системы идентификации по индивидуальным характеристикам человека
9) Организация защищенного документооборота. Виртуальные частные сети
10) Технические каналы утечки акустической информации
11) Защита телефонных разговоров
12) Сертификация средств защиты информации

13) Законодательные основы в области защиты персональных данных
14) Противодействие утечке информации
15) Защита информации в Интернет
16) Технология защиты вычислительной системы от вирусов
17) Криптографические хеш-функции
18) Защита программ от несанкционированного запуска
19) Принципы и методы защиты оптических дисков
20) Парольная защита. Программы-шпионы
21) Криптографические алгоритмы с открытым ключом и их использование
22) Поточные шифры и генераторы псевдослучайных чисел.
23) Простейшие методы шифрования с закрытым ключом
24) Основы защиты авторских прав
25) Электронные деньги.
26) Классификация угроз и объектов защиты
27) Системы контроля доступа и учета рабочего времени
28) Аппаратное шифрование.
29) Социальные методы взлома
30) Защита информации в музыке
31) Защита информации от утечки по техническим каналам
32) Обзор корпоративных межсетевых экранов
33) Обзор алгоритмов ЭЦП
34) Технология BlockChain.
35) Обзор систем обнаружения утечек информации (DLP)
36) Обзор средств защиты в системах интернет-банкинга
37) Лицензирование в области защиты информации: лицензии ФСБ и ФСТЭК
38) Защита персональных данных: закон, подзаконные акты, основные понятия и положения, организационные и технические требования
39) Основные методики оценки рисков информационной безопасности
40) Обзор средств защиты от НСД, имеющих сертификат ФСТЭК
41) Хранение, обработка и уничтожение конфиденциальных документов
42) Обзор стандартов защиты информации: серия стандартов СТО БР ИББС
43) Система сертификации средств защиты информации по требованиям безопасности информации: стандарты, виды и порядок сертификации
44) История развития вирусов и антивирусов, различные виды вирусов.
45) Основные принципы обеспечения информационной безопасности
46) Понятие защищенности автоматизированных систем

47) Меры и средства защиты информации
48) Основы законодательства РФ в области информационной безопасности и защиты информации
49) Лицензирование и сертификация в области обеспечения безопасности информации
50) Международное право в сфере защиты информации
51) Организационное обеспечение информационной безопасности
52) Электромагнитные каналы утечки информации
53) Электрические каналы утечки информации
54) Способы и средства подавления электронных устройств перехвата речевой информации
55) Угрозы безопасности информации, АСОД и субъектов информационных отношений
56) Основные подходы к проектированию систем защиты информации
57) Идентификация, аутентификация и разграничение доступа
58) Методы обнаружения и удаления компьютерных вирусов
59) Симметричные и ассиметричные криптографические системы
60) Классификация угроз безопасности операционных систем
61) Управление целостностью данных
62) Методы воздействий нарушителя на корпоративную сеть
63) Межсетевые экраны
64) Системы обнаружения атак
65) Виртуальные частные сети
66) Информационная безопасность геоинформационных систем
67) Современные средства защиты информации от НСД

Примеры вопросов для собеседования

1. Определение информации.
2. Компьютерные вирусы, их классификация.
3. Виды угроз информации.
4. Алгоритмы шифрования.
5. Криптостойкость.
6. Аутентификация и авторизация.
7. Общая характеристика электромагнитного канала утечки информации
8. Сетевые атаки. Системы обнаружения атак
9. Виды конфиденциальной информации
10. Политика информационной безопасности
11. Основы безопасной работы в Интернет
12. Почему при шифровании методом RSA размер блока увеличивается?

Вопросы для защиты практических работ приведены в соответствующих разделах п.4 основной литературы (У-1).

Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине проводится в форме зачета. Зачет 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.

Примеры типовых заданий для проведения промежуточной аттестации обучающихся:

Задание в закрытой форме:

.....
..... 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.

Задание в открытой форме:

.... Выделяют три основные компоненты информационной системы (указать какие?):

1)……2)…….……3)…….

Задание на установление правильной последовательности,

.... Содержание технологического процесса обработки информации включает ряд процедур. Укажите их правильную последовательность:

- обработка информации;
- хранение;
- сбор;
- визуализация.

Задание на установление соответствия:

Какая технология используется для получения данных из Интернета:

1. файл-сервер; 2. клиент-сервер; 3. Интернет-технология; 4. удаленная технология.

Компетентностно-ориентированная задача:

Приведите процедуру аутентификации пользователя со следующими исходными данными: имя пользователя (Name), пароль (Password), случайное число (V). Процедура перемешивания состоит в последовательном перемешивании полубайтов пароля и случайного числа. Вычисление дайджеста состоит в вычислении остатка перемешенного числа по модулю Password.

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 «О балльно-рейтинговой системе оценивания результатов обучения по дисциплинам (модулям) и практикам при освоении обучающимися 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
Выполнение работы №1 Анализ защищенности вычислительной системы	2	Выполнил, но «не защитил»	2	Выполнил и «защитил»
Выполнение работы №2 Шифры полиалфавитной замены	2	Выполнил, но «не защитил»	3	Выполнил и «защитил»
Выполнение работы №3 Потоковые шифры. Скремблирование бинарного потока данных	2	Выполнил, но «не защитил»	5	Выполнил и «защитил»
Выполнение работы №4 Ассиметричные клиптоалгоритмы. Метод RSA	2	Выполнил, но «не защитил»	8	Выполнил и «защитил»
Выполнение работы №5 Обработка на базе перспективных методов	10	Выполнил, но «не защитил»	10	Выполнил и «защитил»
Выполнение работы №6 Интеграция механизмов защиты в программное обеспечение	4	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Реферат на заданную тему	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
СРС	0		12	
ИТОГО	24		48	
Посещаемость	0		16	
Зачет	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 компетентностно-ориентированной задачи –6 баллов.

Максимальное количество баллов за тестирование - 36 баллов.

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

8.1 Основная литература

1) Технологии обеспечения безопасности информационных систем : учебное пособие : [16+] / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов и др. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с. : ил., схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=598988 (дата обращения: 07.09.2021). – Библиогр.: с. 196-205. – ISBN 978-5-4499-1671-6. – DOI 10.23681/598988. – Текст : электронный.

2) Ищейнов, Вячеслав Яковлевич. Защита конфиденциальной информации [Текст] : учебное пособие / В. Я. Ищейнов, М. В. Мецатунян. - Москва : Форум, 2013. - 256 с.

8.2 Дополнительная литература

3) Организационно-правовое обеспечение информационной безопасности [Текст] : учебное пособие / под ред. А. А. Стрельцова. - М. : Академия, 2008. - 256 с.

4) Романов, О. А. Организационное обеспечение информационной безопасности [Текст] : учебник / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М. : Академия, 2008. - 192 с.

5) Спицын, В. Г. Информационная безопасность вычислительной техники : учебное пособие / В. Г. Спицын ; Томский Государственный университет систем управления и радиоэлектроники (ТУСУР). – Томск : Эль Контент, 2011. – 148 с. – URL: https://biblioclub.ru/index.php?page=book&id=208694 (дата обращения: 27.08.2021). – Режим доступа: по подписке. – Текст : электронный.

8.3 Перечень методических указаний

1) Виды информации и основные методы ее защиты : методические указания по выполнению работы по дисциплине / Юго-Зап. гос. ун-т ; сост. А. Л. Марухленко. - Курск : ЮЗГУ, 2017. - 8 с. - Текст : электронный.

2) Виды угроз информационной безопасности Российской Федерации : методические указания / Юго-Зап. гос. ун-т ; сост. А. Л. Марухленко. - Курск : ЮЗГУ, 2017. - 7 с. - Текст : электронный.

3) Источники угроз информационной безопасности Российской Федерации : методические указания / Юго-Зап. гос. ун-т ; сост. А. Л. Марухленко. - Курск : ЮЗГУ, 2017. - 8 с. - Текст : электронный.

4) Защита от утечек по каналу ПЭМИН, по акустическому и виброакустическому каналам : методические указания по выполнению лабораторной работы по дисциплине / Юго-Зап. гос. ун-т ; сост. А. Л. Марухленко. - Курск : ЮЗГУ, 2017. - 7 с. - Текст : электронный.

5) Анализ трафика и сбор критичной информации программами пассивного анализа : методические указания по выполнению лабораторной работы по дисциплине «Основы информационной безопасности» / Юго-Зап. гос. ун-т ; сост. А. Л. Марухленко. - Курск : ЮЗГУ, 2017. - 6 с. - Текст : электронный.

6) Аудит комплексной защиты информации предприятия : методические указания по выполнению лабораторной работы по дисциплине «Основы информационной безопасности» / Юго-Зап. гос. ун-т ; сост. А. Л. Марухленко. - Курск : ЮЗГУ, 2017. - 8 с. - Текст : электронный.

8. 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)

9. Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Информационная безопасность» являются лекции и практические 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 практические 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.

Практическому 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 практическим работам, а также по результатам докладов.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины: 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 практическим 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”.

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

Microsoft Office 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №K0000000117 от 21.12.2015 г. с ООО «СМСКанал», Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234,Windows, договор IT000012385, Oracle Virtualbox (Бесплатная, GNU General Public License), редактор двоичных файлов Free Hex Editor Neo, (Свободное ПО http://www.hhdsoftware.com/free-hex-editor), портал верификации результатов выполнения практических заданий (https://x46.herokuapp.com) (свободное ПО).

11. 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 на базе CPU AMD-Phenom, ОЗУ 8 GB, HDD 1 Tb, монитор Aok 21” и выше. Проекционный экран на штативе; Мультимедиацентр: ноутбук ASUSX50VLPMD-T2330/14"/1024Mb/160Gb, проектор inFocusIN24+.

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

Компьютерные классы кафедры информационные системы и технологии, оснащены учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска.

Мультимедиа центр: ноутбук ASUSX50VL PMD-T2330/1471024Mb/1 60Gb/

Проектор inFocusIN24+ (39945,45)– 1 шт.

Многофункциональное устройство Canon MF4018 -1 шт.

Многофункциональное устройство Brother MFC-7420R- 3 шт.

Многофункциональное устройство Brother DCP-8065DN- 1 шт.

Принтер 3D UP - 1 шт.

Компьютерный класс а-214.

Компьютер ВАРИАНТ PDC2160/iC33/2*512Mb/ HDD160Gb/DVD-ROM/FDD/ATX350W/K/m/WXP/0 FF/17"TFTE700 (18809.20) – 10 шт;

Вычислительный комплекс имитационного моделирования – 3 шт;

Компьютерный класс а-207

Компьютер IntelCore i3-4330, 3.5GHz, 8Gb, 500Gb HDD, LCD Philips 21”– 10 шт;

13 Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.). Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).

14 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			