Аннотация к рабочей программе дисциплины «Комплексное обеспечение информационной безопасности инфокоммуникационных систем»

Цель преподавания дисциплины

Дисциплина «Комплексное обеспечение информационной безопасности инфокоммуникационных систем» является получение студентами знаний о принципах построения, идеологии и архитектуре современных операционных систем, реализуемых в них механизмах защиты.

Задачи изучения дисциплины

В результате изучения дисциплины студенты должны:

1) получить знания о назначении, принципах функционирования и структуре операционных систем;

2)получить знания о функционировании подсистемы управления процессами;

3) получить знания о функционировании подсистем управления распределением ресурсов

4) получить знания о функционировании подсистем управления памятью в различных операционных системах;

5) получить знания о назначении, организации и функционировании файловых систем;

6)получить знания о функционировании подсистемы устройствами ввода – вывода;

7) получить знания о принципах организации операционных систем семейств Windows и UNIX

8) получить знания о методах и средствах оценки производительности операционных систем, загруженности системных ресурсов.

9) получить знания о механизмах защиты объектов, реализованных средствами операционной системы Windows.

Компетенции, формируемые в результате освоения дисциплины

Способность организовывать работу малых коллективов исполнителей, принимать управленческие решения в сфере профессиональной деятельности, разрабатывать предложения по совершенствованию системы управления информационной безопасностью телекоммуникационной системы (ПК-11);

Способность оценивать возможности средств технических разведок в отношении к системам связи, управления и объектам информатизации (ПК-10.3).

Разделы дисциплины

Понятие ОС, история, классификация, основные функции. Процессы, модель, состояния. Процессы, модель, состояния. Нити. Диспетчеризация и синхронизация процессов. Проблемы межпроцессного взаимодействия. Взаимоблокировки процессов. Управление памятью в ОС. Механизмы разграничения доступа в ОС. Механизмы безопасной работы в ОС. Администрирование ОС.

МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
Декан факультета
фундаментальной и прикладной
(наименование ф-та полностью)
информатики
Т.А. Ширабакина
(подпись, инициалы, фамилия)
«1» февраля 2017 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Комплексное обеспечение информационной безопасности инфокоммуникационных систем

направление подготовки (специальность) 10.05.02
(шифр согласно ФГОС
Информационная безопасность телекоммуникационных систем
и наименование направление подготовки (специальности)

«Защита информации в системах связи и управления»
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 10.05.02 – «Информационная безопасность телекоммуникационных систем» и на основании учебного плана подготовки специалистов по специальности 10.05.02 – «Информационная безопасность телекоммуникационных систем», одобренного Учёным советом университета, протокол № 5 «30» 01 2017 г.

Рабочая программа обсуждена и рекомендована к применению в учебном процессе для обучения студентов по специальности 10.05.02 – «Информационная безопасность телекоммуникационных систем» на заседании кафедры информационной безопасности.
«1» февраля 2017 г. Протокол № 9

И.о. зав. кафедрой ИБ Таныгин М.О.

Разработчик программы
доцент кафедры ИБ Карасовский В.В.

Согласовано:
Директор научной библиотеки Макаровская В.Г.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана по специальности 10.05.02 – «Информационная безопасность телекоммуникационных систем», одобренного Ученым советом университета протокол № 5 «30» 01 2017 г. на заседании кафедры. протокол №1 от 28.08.17
Зав. кафедрой Таныгин М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана по специальности 10.05.02 – «Информационная безопасность телекоммуникационных систем», одобренного Ученым советом университета протокол № 5 «30» 01 2017 г. на заседании кафедры. ИБ, протокол №12 от 29.06.18 г.
Зав. кафедрой Таныгин М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана по специальности 10.05.02 – «Информационная безопасность телекоммуникационных систем», одобренного Ученым советом университета протокол №___ «___» _____ 20__ г. на заседании кафедры, Информационной безопасности 27.06.2019 №11
Зав. кафедрой КТН, доцент Таныгин М.О.

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.05.02 – «Информационная безопасность телекоммуникационных систем»*, одобренного Ученым советом университета протокол №_7_ «_25_» _02_ 20_20_ г. на заседании кафедры информационной безопасности. Протокол №_1_ от «_31_» _08_ 20_20_г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.05.02 – «Информационная безопасность телекоммуникационных систем»*, одобренного Ученым советом университета протокол №_7_ «_25_» _02_ 20_20_ г. на заседании кафедры информационной безопасности. Протокол №_11_ от «_28_» _06_ 20_21_г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.05.02 – «Информационная безопасность телекоммуникационных систем»*, одобренного Ученым советом университета протокол №_7_ «_25_» _02_ 20_20_ г. на заседании кафедры информационной безопасности. Протокол №_11_ от «_30_» _06_ 20_22_г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.05.02 – «Информационная безопасность телекоммуникационных систем»*, одобренного Ученым советом университета протокол №__ «___» _____ 20__ г. на заседании кафедры информационной безопасности. Протокол №__ от «__»_____20__г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.05.02 – «Информационная безопасность телекоммуникационных систем»*, одобренного Ученым советом университета протокол №__ «___» _____ 20__ г. на заседании кафедры информационной безопасности. Протокол №__ от «__»_____20__г.

Зав. кафедрой _____

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

Цель дисциплины

Целью преподавания дисциплины «Комплексное обеспечение информационной безопасности инфокоммуникационных систем» является изучение структур, организаций и принципов функционирования комплексных систем защиты информации (КСЗИ) инфокоммуникационных систем.

Задачи дисциплины

Основными обобщенными задачами дисциплины являются:

- раскрытие сущности, целей и задач КСЗИ;
- определение принципов и этапов разработки КСЗИ;
- освоение технологии установления состава защищаемой информации и объектов защиты;
- овладение методами оценки уязвимости защищаемой информации;
- определение параметров и структуры КСЗИ;
- установление состава мероприятий по обеспечению функционирования КСЗИ;
- раскрытие структуры и методов управления КСЗИ;
- определение показателей эффективности КСЗИ и методики ее оценки.

1.3 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Обучающиеся должны **знать:**

- основные понятия, цели и задачи КСЗИ инфокоммуникационных систем;
- сущность и составляющие КСЗИ;
- принципы организации и этапы разработки КСЗИ;
- факторы, влияющие на организацию КСЗИ;
- технологию определения состава защищаемой информации и объектов защиты;
- методы анализа и оценки угроз защищаемой информации в инфокоммуникационных системах;
- технологическое и организационное построение КСЗИ;
- состав мероприятий и условия, обеспечивающие функционирование КСЗИ;
- технологию управления КСЗИ;
- методику проведения анализа эффективности функционирования

КСЗИ;

уметь:

– определять состав защищаемой информации и объектов защиты;

– выявлять угрозы защищаемой информации, определять степень их опасности;

– разрабатывать структуру КСЗИ с учетом условий ее функционирования;

– определять состав защитных мероприятий;

– определять состав кадрового, нормативно-методического и материально-технического обеспечения функционирования КСЗИ;

– выбирать методы и средства, необходимые для организации и функционирования КСЗИ;

– разрабатывать планы функционирования КСЗИ;

– осуществлять текущее руководство функционированием КСЗИ;

– обеспечить взаимодействие персонала, реализовывающего функционирование КСЗИ;

– анализировать эффективность КСЗИ;

владеть :

– определения требований и состава средств, методов и мероприятий по организации КСЗИ;

– использования методов организации, планирования и контроля функционирования КСЗИ;

– разработки организационно-функциональной структуры и комплекса нормативно-методического обеспечения КСЗИ;

– проведения оценки качества функционирования различных компонентов КСЗИ.

У обучающихся формируются следующие компетенции:

– способность применять технологии обеспечения информационной безопасности телекоммуникационных систем и нормы их интеграции в государственную и международную информационную среду (ПК-6);

– способность организовывать работу малых коллективов исполнителей, принимать управленческие решения в сфере профессиональной деятельности, разрабатывать предложения по совершенствованию системы управления информационной безопасностью телекоммуникационной системы (ПК-11);

– способность оценивать возможности средств технических разведок в отношении к системам связи, управления и объектам информатизации (ПК-10.3).

2. Указание места дисциплины в структуре образовательной программы

Дисциплина относится к дисциплинам вариативной части профессионального цикла (Б1.В.ОД.10). Изучается на 5 курсе в 10 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 6 зачётных единиц, 216 часов

Таблица 3.1 – Объём дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	216
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	72,15
Лекции	36
лабораторные занятия	18
практические занятия	18
экзамен	0,15
зачет	-
курсовая работа (проект)	не предусмотрено
расчетно-графическая (контрольная) работа	не предусмотрено
Аудиторная работа (всего):	36
в том числе:	
лекции	36
лабораторные занятия	18
практические занятия	18
Самостоятельная работа обучающихся (всего)	90
Контроль/экз (подготовка к экзамену)	36

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	2	3
1.	Сущность и задачи комплексной системы защиты информации.	Понятие и сущность КСЗИ. Назначение КСЗИ. Задачи КСЗИ. КСЗИ как средство выражения концептуальных основ защиты информации. Классификация методов и средств защиты информации Методология защиты информации как теоретический базис построения КСЗИ Периметра и здания предприятия. Специфика персонала предприятия как объекта защиты.
2.	Принципы организации и этапы разработки комплексной системы защиты информации.	Методологические основы организации КСЗИ. КСЗИ как сложная человеко-машинная система. Основные положения теории систем. Принципы организации КСЗИ. Основные требования, предъявляемые к КСЗИ. Содержательная

		характеристика этапов разработки КСЗИ. Основные факторы, влияющие на организацию КСЗИ: организационно-правовая форма и характер основной деятельности предприятия; состав, объем и степень конфиденциальности защищаемой информации; структура и территориальное расположение предприятия; режим функционирования предприятия; конструктивные особенности предприятия; количественные и качественные параметры ресурсообеспечения; степень автоматизации основных процедур обработки защищаемой информации. Характер и степень влияния различных факторов на организацию КСЗИ.
3.	Определение и нормативное закрепление состава защищаемой информации.	Методика определения состава защищаемой информации. Этапы работы по выявлению состава защищаемой информации. Функции руководства предприятия и подразделений предприятия, экспертной комиссии, службы защиты информации. Классификация информации по видам тайны и степеням конфиденциальности. Нормативное закрепление состава защищаемой информации; структура перечней сведений, относимых к различным видам тайны. Порядок внедрения перечней, внесения в них изменений и дополнений
4.	Определение объектов защиты.	Значение носителей защищаемой информации как объектов защиты Факторы, определяющие состав носителей информации. Методика выявления состава носителей защищаемой информации. Хранилища носителей информации как объект защиты. Особенности помещений для работы с защищаемой информацией как объектов защиты. Состав технических средств обработки, передачи, транспортировки и защиты информации, являющихся объектами защиты. Состав средств обеспечения функционирования предприятия, подлежащих защите. Факторы, определяющие необходимость защите
5.	Выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию.	Методика выявления каналов несанкционированного доступа к информации. Соотношение между каналами несанкционированного доступа и источниками воздействия на информацию. Определение возможных методов несанкционированного доступа к защищаемой информации. Оценка степени опасности применения различных методов. Анализ потенциальных последствий реализации несанкционированного доступа. Методика выявления нарушителей (незаконных пользователей) и состава интересующей их информации. Определение направлений и возможностей доступа нарушителей к защищаемой информации. Оценка степени уязвимости информации в результате действий нарушителей различных категорий.
6.	Определение компонентов комплексной системы защиты информации.	Факторы, влияющие на выбор компонентов КСЗИ. Объекты защиты как основной фактор, определяющий состав компонентов КСЗИ. Основные требования, предъявляемые к выбору методов и средств защиты, зависимость их от структуры предприятия, защищаемых элементов объектов, условий функционирования КСЗИ. Обеспечение полноты составляющих защиты. Учет всех факторов и обстоятельств,

		оказывающих влияние на качество защиты. Обеспечение безопасности всей совокупности подлежащей защите информации во всех компонентах ее сбора, хранения, передачи и использования, а также в течении всего времени и при всех режимах функционирования систем обработки информации.
7.	Разработка модели комплексной системы защиты информации.	Понятие модели объекта, основные виды моделей и их характеристика. Модель как инструмент количественного и качественного анализа КСЗИ. Значение моделирования процессов КСЗИ. Выбор структуры КСЗИ, ее зависимость от объектов защиты, характера и условий функционирования предприятия. Функциональная модель КСЗИ. Организационная модель КСЗИ. Информационная модель КСЗИ.
8.	Технологическое и организационное построение комплексной системы защиты информации.	Общее содержание работ по организации КСЗИ. Характеристика основных стадий создания КСЗИ. Назначение и структура задания на проектирование, технического задания, технико-экономического обоснования. Предпроектное обследование, технический проект, рабочий проект. Апробация и ввод в эксплуатацию.
9.	Назначение, структура и содержание управления комплексной системой защиты информации.	Понятие и цели управления КСЗИ. Сущность процессов управления ССЗИ. Принципы управления КСЗИ. Основные стили управления. Структура и содержание общей технологии управления КСЗИ.

Таблица 4.2– Содержание дисциплины и ее методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		лек., час	№ пр.	№лб.			
1	2	3	4	5	6	7	8
1.	Сущность и задачи комплексной системы защиты информации.	4		1	У-1 МУ-1,3	С	ПК-6
2.	Принципы организации и этапы разработки комплексной системы защиты информации.	4		2	У-1,2, МУ-1,4	С	ПК-6, ПК-11
3.	Определение и нормативное закрепление состава защищаемой информации.	4			У-1,3 МУ-1	С	ПК-6, ПК-11
4.	Определение объектов защиты.	4	1		У-1,4 МУ-1,2	С	ПК-6, ПК-10.3
5.	Выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию.	4		3	У-2,3 МУ-1,5	С	ПК-6, ПК-10.3

1	2	3	4	5	6	7	8
6.	Определение компонентов комплексной системы защиты информации.	4	2		У-1,2,3 МУ-1,2	С	ПК-6, ПК-10.3
7.	Разработка модели комплексной системы защиты информации.	4	3		У-2-6, МУ-1,2	С	ПК-6
8.	Технологическое и организационное построение комплексной системы защиты информации.	4	4		У-1,3,4, МУ-1,2	С	ПК-6, ПК-11
9.	Назначение, структура и содержание управления комплексной системой защиты информации.	4		4	У-1,3,4, МУ-1,6	С	ПК-6, ПК-11

С – собеседование.

4.2 Лабораторные работы и (или) практические занятия

4.2.1 Лабораторные работы

Таблица 4.3 – Лабораторные работы

№	Наименование лабораторной работы	Объем, час.
1.	Демаскирующие признаки объекта	4
2.	Изучение существующих каналов утечки информации	4
3.	Определение показателей защищенности информации при несанкционированном доступе	6
4.	Оценка показателей качества функционирования комплексной системы защиты информации на предприятии: физическое проникновение	4
Итого		18

4.2.2 Практические занятия

Таблица 4.4 – Практические занятия

№	Наименование практической работы	Объем, час.
1.	Моделирование объектов защиты	4
2.	Моделирование угроз безопасности информации	4
3.	Разработка организационных и технических мер по инженерно-технической защите информации	6
4.	Выбор средств защиты информации	4
Итого		18

Самостоятельная работа студентов (СРС)

Таблица 4.5 – Самостоятельная работа студентов

№	Наименование раздела учебной дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.

1.	Сущность и задачи комплексной системы защиты информации.	1-2 неделя	10
2.	Принципы организации и этапы разработки комплексной системы защиты информации.	3-4 неделя	10
3.	Определение и нормативное закрепление состава защищаемой информации.	5-6 неделя	10
4.	Определение объектов защиты.	7-8 неделя	10
5.	Выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию.	9-10 неделя	10
6.	Определение компонентов комплексной системы защиты информации.	11-12 неделя	10
7.	Разработка модели комплексной системы защиты информации.	13-14 неделя	10
8.	Технологическое и организационное построение комплексной системы защиты информации.	15-16 неделя	10
9.	Назначение, структура и содержание управления комплексной системой защиты информации.	17-18неделя	10
Итого			90

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 за счёт выкладывания на сайт кафедры ИБ в интернете (адрес http://www.swsu.ru/structura/up/fivt/k_ib/index.php);

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

– путем разработки вопросов к экзамену

– методических указаний к выполнению практических и лабораторных работ.

типографией университета

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

Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине из числа инвалидов и лиц с ограниченными возможностями здоровья предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в печатной форме увеличенным шрифтом,
- в форме электронного документа,

Для лиц с нарушениями опорно-двигательного аппарата:

- в печатной форме,
- в форме электронного документа

6. Образовательные технологии

В соответствии с требованиями ФГОС и Приказа Министерства образования и науки РФ от 05 апреля 2017 г. №301 реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков студентов. Удельный вес занятий, проводимых в интерактивных формах, составляет 25.2% от аудиторных занятий согласно УП. Средствами промежуточного контроля успеваемости студентов являются защита лабораторных работ, опросы на практических занятиях по темам лекций.

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

№	Наименование раздела (темы лекции, практического или лабораторного занятия)	Используемые интерактивные образовательные технологии	Объём, час.
1.	Выполнение практической работы №1 «Моделирование объектов защиты».	Разбор конкретных ситуаций	4
2.	Выполнение практической работы №2 «Моделирование угроз безопасности информации».	Разбор конкретных ситуаций	4
3.	Выполнение практической работы №4 «Выбор средств защиты информации»	Формирование актуального перечня средств защиты информации для индивидуального варианта задания	4
4.	Выполнение лабораторной работы №1 «Демаскирующие признаки объекта».	Определение и обоснование выбора демаскирующих признаков для информационной системы	4
5.	Выполнение лабораторной работы №2 «Изучение существующих каналов утечки информации».	Определение характеристик каналов утечки конфиденциальной информации	4
6.	Выполнение лабораторной работы	Формирование критериев и	4

	№4 «Оценка показателей качества функционирования комплексной системы защиты информации на предприятии: физическое проникновение»	использование их для оценки качества комплексной системы защиты информации	
	Итого		24

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

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

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 технологии обеспечения информационной безопасности телекоммуникационных систем и нормы их интеграции в государственную и международную информационную среду (ПК-6)			Защита информации в системах беспроводной связи Комплексное обеспечение информационной безопасности инфокоммуникационных систем Безопасность распределенных баз данных Безопасность систем и сетей передачи данных Конструкторская практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты
Способность организовывать работу малых коллективов исполнителей, принимать управленческие решения в сфере профессиональной деятельности, разрабатывать предложения по совершенствованию системы управления информационной безопасностью телекоммуникационной системы (ПК-11)	Психология Психология управления коллективом	Социология Основы социологических исследований	Основы управленческой деятельности Эксплуатационная практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты

Способность оценивать возможности средств технических разведок в отношении к системам связи, управления и объектам информатизации (ПСК-10.3)		Техническая защита информации Комплексное обеспечение информационной безопасности инфокоммуникационных систем Конструкторская практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты

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

Наименование компетенции	Критерии освоения		
	Пороговый уровень («удовлетворительно»)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
Способность применять технологии обеспечения информационной безопасности телекоммуникационных систем и нормы их интеграции в государственную и международную информационную среду (ПК-6)	**Знать:** перечень технологий обеспечения информационной безопасности **Уметь:** выполнять процессы интеграции технологий обеспечения информационной безопасности в комплексную систему обеспечения информационной безопасности ТКС **Владеть навыками:** использования технологий обеспечения информационной безопасности	**Знать:** технологии обеспечения информационной безопасности и их назначение. **Уметь:** использовать технологии обеспечения информационной безопасности в рамках работы комплексной системы обеспечения информационной безопасности ТКС . **Владеть навыками:** выполнения технологических операций обеспечения информационной безопасности;	**Знать:** технологии обеспечения информационной безопасности, их назначение, особенности применения в конкретных ситуациях. **Уметь:** использовать технологии обеспечения информационной безопасности для реализации комплексной системы обеспечения информационной безопасности ТКС .; **Владеть навыками:** обеспечения комплексной информационной безопасности ТКС .
Способность организовывать	**Знать**: основные положения и нормы	**Знать**: организационную	**Знать**: принципы принятия

работу малых коллективов исполнителей, принимать управленческие решения в сфере профессиональной деятельности, разрабатывать предложения по совершенствовани ю системы управления информационной безопасностью телекоммуникацио нной системы (ПК-11)	конституционного, гражданского, трудового права **Уметь**: сопоставлять организационную структуры комплексной и стремы обеспечения информационной безопасности требованиям законодательства **Владеть навыками**: Формирования организационных решений в области обеспечения ИБ	структуру комплексной системы обеспечения безопасности ТКС **Уметь**: формулировать должностные обязанности сотрудников, обеспечивающих комплексную безопасность ТКС **Владеть навыками**: Формирования организационной структуры системы комплексной защиты информации	управленческих решений в области ИБ **Уметь**: сопоставлять задачи и методы обеспечения ИБ должностным обязанностям сотрудников; **Владеть навыками**: Принятия управленческих решений в области ИБ;
Способность оценивать возможности средств технических разведок в отношении к системам связи, управления и объектам информатизации (ПК-10.3)	**Знать** систему мер противодействия промышленному шпионажу **Уметь**: формулировать угрозы ТКС со стороны технических разведок; **Владеть навыками**: Анализа угроз информационной безопасности ТКС;	**Знать** дополнительно активные и пассивные методы сбора информации **Уметь**: формировать перечень мер противодействия техническим разведкам; **Владеть навыками**: Сопоставления структуры и функционала компонентов ТКС методам возможного воздействия со стороны технических разведок;	**Знать** возможности технических разведок **Уметь**: использовать организационные, аналитические, технические средства противодействия техническим разведкам ; **Владеть навыками**: Анализа возможности средств технических разведок в отношении к системам связи.

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине обеспечивается выполнение следующих дополнительных требований в зависимости от индивидуальных особенностей обучающихся: а) инструкция по порядку проведения процедуры оценивания предоставляется в доступной форме (устно, в письменной форме);

б) доступная форма предоставления заданий оценочных средств (в печатной форме, в печатной форме увеличенным шрифтом, в форме электронного документа, задания зачитываются ассистентом);
в) доступная форма предоставления ответов на задания (письменно на бумаге, набор ответов на компьютере, с использованием услуг ассистента, устно).
При необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

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 форматирования	Оценочные средства		Описание шкал оценивания
				наимено-вание	№ заданий	
1	2	3	4	5	6	7
1	Сущность и задачи комплексной системы защиты информации.	ПК-6	Лекция, лабораторная работа, СРС	Собесе-дование		Согласно табл. 7.2
				Контрольные вопросы к ЛР №1		
2	Принципы организации и этапы разработки комплексной системы защиты информации.	ПК-6, ПК-11	Лекция, лабораторная работа, СРС	Собеседование		Согласно табл. 7.2
				Контрольные вопросы к ЛР №2		
3	Определение и нормативное закрепление состава защищаемой информации.	ПК-6, ПК-11	Лекция, СРС	Собесе-дование		Согласно табл. 7.2
4	Определение объектов защиты.	ПК-6, ПК-10.3	Лекция, СРС, практическая работа	Собесе-дование,		Согласно табл. 7.2
				Контрольные вопросы к ПР №1	1-5	
5	Выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию.	ПК-6, ПК-10.3	Лекция, лабораторная работа, СРС	Собесе-дование		Согласно табл. 7.2
				Контрольные вопросы к ЛР №3		

6	Определение компонентов комплексной системы защиты информации.	ПК-6, ПК-10.3	Лекция, СРС, практическая работа	Собесе-дование		Согласно табл. 7.2
				Контрольные вопросы к ПР №2	1-5	
7	Разработка модели комплексной системы защиты информации.	ПК-6	Лекция, СРС, практическая работа	Собесе-дование		Согласно табл. 7.2
				Контрольные вопросы к ПР №3	1-5	
8	Технологическое и организационное построение комплексной системы защиты информации	ПК-6, ПК-11	Лекция, СРС, практическая работа	Собесе-дование		Согласно табл. 7.2
				Контрольные вопросы к ПР №4	1-5	
9	Назначение, структура и содержание управления комплексной системой защиты информации.	ПК-6, ПК-11	Лекция, СРС, лабораторная работа	Собесе-дование		
				Контрольные вопросы к ЛР №4		

Примеры типовых контрольных заданий для текущего контроля

Вопросы для собеседования

Принципы организации и этапы разработки комплексной системы защиты информации.

1. Методологические основы организации КСЗИ.
2. Принципы организации КСЗИ.
3. Основные требования, предъявляемые к КСЗИ.
4. Этапы разработки КСЗИ.
5. Основные факторы, влияющие на организацию КСЗИ
6. Характер и степень влияния различных факторов на организацию КСЗИ

7.4 Рейтинговый контроль изучения учебной дисциплины

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

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

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

Для *текущего контроля* по дисциплине в рамках действующей в университете бально-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 практической работы №1 «Моделирование объектов защиты».	3	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Выполнение практической работы №2 «Моделирование угроз безопасности информации».	3	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Выполнение практической работы №3 «Разработка организационных и технических мер по инженерно-технической защите информации»	3	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Выполнение практической работы №4 «Выбор средств защиты информации»	3		4	
Выполнение лабораторной работы №1 «Демаскирующие признаки объекта»	3	Выполнил, но «не защитил»	5	Выполнил и «защитил»
Выполнение лабораторной работы №2 «Изучение существующих каналов утечки информации»	3	Выполнил, но «не защитил»	5	Выполнил и «защитил»
Выполнение лабораторной работы №3 «Определение показателей защищенности информации при несанкционированном доступе»	3	Выполнил, но «не защитил»	5	Выполнил и «защитил»
Выполнение лабораторной работы №4 «Оценка показателей качества функционирования комплексной системы защиты информации на предприятии: физическое проникновение»	3	Выполнил, но «не защитил»	5	Выполнил и «защитил»
СРС	0		12	
Итого	24		48	
Посещаемость	0		16	
Экзамен	0		36	
Итого	24		100	

При итоговом контроле (экзамен) в форме бланкового теста студенту предлагается 15 вопросов по различным темам курса. Полученную итоговую сумму условных баллов (максимум 15) переводят в баллы на экзамене (максимум 36) путём умножения на 2.4 и округления до целого значения. Пример билета в тестовой форме приведён в приложении В

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

8.1 Основная учебная литература

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

2. Информационная безопасность и защита информации [Текст] : учебное пособие / Ю. Ю. Громов [и др.]. - Старый Оскол : ТНТ, 2013. - 384 с. - ISBN 978-5-94178-2 16-1

3. Сердюк, В. А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий [Электронный ресурс] : учебное пособие / В. А. Сердюк ; Высшая Школа Экономики Национальный Исследовательский Университет. - М. : Издательский дом Высшей школы экономики, 2015. - 574 с. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=440285

8.2 Дополнительная литература

Грекул, В. И. Проектирование информационных систем [Электронный ресурс] : курс лекций : учебное пособие / В. И. Грекул, Г. Н. Денищенко, Н. Л. Коровкина. - М.: Интернет-Университет Информационных Технологий, 2005. – 304 с. - http://biblioclub.ru/index.php?page=book&id=233071

5. Лопин, В. Н. Защита информации в компьютерных системах [Текст] : учебное пособие / В. Н. Лопин, И. С. Захаров, А. В. Николаев ; Министерство образования и науки Российской Федерации, Курский государственный технический университет. - Курск : КГТУ, 2006. - 159 с.

6. Гусева, А. И. Сети и межсетевые коммуникации: Windows 2000 [Электронный ресурс] : учебник / А. И. Гусева. - М. : Диалог-МИФИ, 2002. - 257 с. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=136075

7. Болодурина, И. П. Системный анализ [Электронный ресурс] : учебное пособие / И. Болодурина, Т. Тарасова, О. Арапова ; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Оренбургский государственный университет». - Оренбург : ОГУ, 2013. - 193 с. — Режим доступа: http://biblioclub.ru/index.php?page=book&id=259157

8. Шапкин, А .С. Математические методы и модели исследования операций [Электронный ресурс] : учебник / А. С. Шапкин, В. А. Шапкин. - 7-е изд. - М. : Издательско-торговая корпорация «Дашков и К°», 2017. - 398 с. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=452649

8.2 Перечень методических указаний

1) Комплексное обеспечение информационной безопасности инфокоммуникационных систем: методические указания к СРС / сост.: Таныгин М.О. Электрон. текстовые дан. - Курск : Юго-Зап. гос. ун-т ;, 2018. - 10 с. : ил., табл. - Библиогр.: с. 9. - Б. ц.

2) Комплексное обеспечение информационной безопасности инфокоммуникационных систем: методические указания к практическим занятиям / сост.: Калуцкий И.В., Чеснокова А.А., Таныгин М.О. Электрон. текстовые дан. - Курск : Юго-Зап. гос. ун-т ;, 2017. - 48 с. : ил., табл. - Библиогр.: с. 48. - Б. ц.

3) Демаскирующие признаки объекта [Электронный ресурс] : методические указания по выполнению лабораторных и практических работ : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: Калуцкий И.В., Куденцова Ю.А. - Электрон. текстовые дан. - Курск : ЮЗГУ, 2017. - 12 с. : ил., табл. - Библиогр.: с. 12. - Б. ц

4) Демаскирующие признаки объекта [Электронный ресурс] : методические указания по выполнению лабораторных и практических работ : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: Калуцкий И.В., Куденцова Ю.А. - Электрон. текстовые дан. - Курск : ЮЗГУ, 2017. - 12 с. : ил., табл. - Библиогр.: с. 12. - Б. ц.

5) Изучение существующих каналов утечки информации [Электронный ресурс] : методические указания по выполнению лабораторных и практических работ : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: Калуцкий И.В., Куденцова Ю.А. - Электрон. текстовые дан. - Курск : ЮЗГУ, 2017. - 12 с. : ил., табл. - Библиогр.: с. 12. - Б. ц.

6) Определение показателей защищенности информации при несанкционированном доступе [Электронный ресурс] : методические указания по выполнению лабораторной работы : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: В. В. Карасовский, О. А. Демченко. - Электрон. текстовые дан. (342 КБ). - Курск : ЮЗГУ, 2017. - 7 с. : ил., табл. - Библиогр.: с. 7. - Б. ц.

7) Оценка показателей качества функционирования комплексной системы защиты информации на предприятии: физическое проникновение [Электронный ресурс] : методические указания по выполнению лабораторной работы : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: В. В. Карасовский, О. А. Демченко. - Электрон. текстовые дан. (541 КБ). - Курск : ЮЗГУ, 2017. - 16 с. : ил., табл. - Библиогр.: с. 16. - Б. ц.

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) Электронно-библиотечная система «Университетская библиотека онлайн» Режим доступа: http://biblioclub.ru
4) Компания «Консультант Плюс» [официальный сайт]. Режим доступа: http://www.consultant.ru
5) Научно-информационный портал ВИНИТИ РАН [официальный сайт]. Режим доступа: http://www.consultant.ru/
6) База данных "Патенты России"
7) Аналитический раздел компании «Код Безопасности» https://www.securitycode.ru/documents/analytics/

10. Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Комплексное обеспечение информационной безопасности инфокоммуникационных систем» являются лекции и практические работы. 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 и лабораторные работы, 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.

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

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

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Комплексное обеспечение информационной безопасности инфокоммуникационных 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.

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, знакомиться с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Комплексное обеспечение информационной безопасности инфокоммуникационных систем» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Комплексное обеспечение информационной безопасности инфокоммуникационных систем»: конспектирование учебной литературы и лекции, составление словарей» - закрепить теоретические знания, полученные в процессе лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

11. 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 7, договор IT000012385

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

Учебная аудитория для проведения занятий лекционного и практического типа или лаборатории кафедры «информационная

безопасность», оснащенные мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска, проектор для демонстрации презентаций. Помещение для самостоятельной работы Компьютер PDC2160/iC33/2*512Mb/HDD 160Gb/DVD-ROM/FDD/ATX350W/ K/m/ OFF/l 7"TFT E700 (6 шт)

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			
1		4, 14			2	23.08.18	Приказ ректора от 23.08.18 № 90