Аннотация к рабочей программе дисциплины «Работа с конфиденциальной информацией»

Цель преподавания дисциплины

Целью преподавания дисциплины «Работа с конфиденциальной информацией» является приобретение студентами знаний по работе с конфиденциальной информацией в организациях и предприятиях различных направлений деятельности и различных форм собственности и формирование практических навыков работы в реальных конкретных условиях.

Задачи изучения дисциплины

– научить студентов в конкретных условиях анализировать наиболее значимые аспекты безопасности создания, формирования, жизненного цикла и документопотоков конфиденциальной информации;

– изучение основных методов организационной защиты конфиденциальных документов;

– научить студентов осуществлять правильный выбор организационных форм защиты конфиденциальной информации в зависимости от ее вида, ценности, объема, и способа представления, а также в зависимости от стоимости используемых технических средств, удобства их использования и надежности функционирования;

– изучение основных нормативно-правовых актов, регламентирующих защиту и обработку конфиденциальных документов.

Компетенции, формируемые в результате освоения дисциплины

Способен использовать основы правовых знаний в различных сферах деятельности (ОК-4);

Способен использовать нормативные правовые акты в профессиональной деятельности (ОПК-5);

Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10);

Способен организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ПК-15).

Разделы дисциплины

Организационные и правовые основы обеспечения безопасности конфиденциальной информации. Организационные источники и каналы утечки информации. Технические и программные средства защиты информации. Коммерческая тайна и порядок её определения. Организация работ с информацией, составляющей коммерческую тайну. Подбор персонала на должности, связанные с работой с информацией ограниченного доступа. Организация деятельности службы безопасности объекта. Организация внутриобъектового режима. Требования, предъявляемые к помещениям и хранилищам, в которых ведутся закрытые работы, хранятся документы ограниченного доступа и изделия. Организация защиты информации при приеме в организации посетителей командированных лиц и иностранных представителей. Организация проведения служебного расследования по фактам разглашения сотрудниками информации ограниченного доступа. Охрана объектов. Организация защиты информации при подготовке и проведению совещаний и переговоров. Организация защиты информации при осуществлении научно-публицистической деятельности. Защита информации при рекламной деятельности. Основные принципы организации аналитической работы служб безопасности по недопущению утечки конфиденциальной информации. Подготовка лиц, ответственных за обеспечение безопасности информации.

Содержание основных методов и работы с персоналом, обладающим конфиденциальной информацией.

МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Работа с конфиденциальной информацией

направление подготовки (специальность) *10.03.01*
(шифр согласно ФГОС
Информационная безопасность
и наименование направление подготовки (специальности)

Безопасность автоматизированных систем
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 профессионального образования направления подготовки *10.03.01 – «Информационная безопасность»* и на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Учёным советом университета, протокол «30» 01 2017 г.

Рабочая программа обсуждена и рекомендована к применению в учебном процессе для обучения студентов по направлению подготовки *10.03.01 – «Информационная безопасность»* на заседании кафедры информационной безопасности.

«1» февраля 2017 г. Протокол № 9

Зав. кафедрой ИБ Таныгин М.О.

Разработчик программы
доцент кафедры ИБ Таныгин М.О.

Согласовано:
Директор научной библиотеки Макаровская В.Г.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана по специальности *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол № 5 «30» 01 2017 г. на заседании кафедры информационной безопасности. Протокол № 1 «28» 08 2017 г.

Зав. кафедрой Таныгин М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана по специальности *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол № 5 «30» 01 2018 г. на заседании кафедры информационной безопасности. Протокол № 12 «29» 06 2018 г.

Зав. Кафедрой Таныгин М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана по специальности *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол № «» 20 г. на заседании кафедры информационной безопасности. Протокол № 11 «27» 06 2019 г.

Зав. кафедрой Таныгин М.О.

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №7 «25» 02 2020 г. на заседании кафедры информационной безопасности. Протокол №1 от «31» 08 2020г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №7 «25» 02 2020 г. на заседании кафедры информационной безопасности. Протокол №11 от «28» 06 2021 г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №7 «25» 02 2020 г. на заседании кафедры информационной безопасности. Протокол №11 от «30» 06 2022 г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, 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 *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №__ «___» _____ 20__ г. на заседании кафедры информационной безопасности. Протокол №__ от «__»_____20__г.

Зав. кафедрой _____

1. Цель и задачи дисциплины, планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

1.1. Цель дисциплины

Целью преподавания дисциплины «Работа с конфиденциальной информацией» является приобретение студентами знаний по работе с конфиденциальной информацией в организациях и предприятиях различных направлений деятельности и различных форм собственности и формирование практических навыков работы в реальных конкретных условиях.

1.2. Задачи изучения дисциплины

- научить студентов в конкретных условиях анализировать наиболее значимые аспекты безопасности создания, формирования, жизненного цикла и документопотоков конфиденциальной информации;
- изучение основных методов организационной защиты конфиденциальных документов;
- научить студентов осуществлять правильный выбор организационных форм защиты конфиденциальной информации в зависимости от ее вида, ценности, объема, и способа представления, а также в зависимости от стоимости используемых технических средств, удобства их использования и надежности функционирования;
- изучение основных нормативно-правовых актов, регламентирующих защиту и обработку конфиденциальных документов.

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

знать:

- методы анализа изучаемых явлений, процессов и проектных решений;
- основные правила организации технологического процесса защиты информации ограниченного доступа;
- требования стандартов в области информационной безопасности;
- номенклатуру и характеристики средств обеспечения сетевой безопасности;

уметь:

- проводить предварительный технико-экономический анализ и обосновать проектные решения по обеспечению информационной безопасности;
- формировать комплект документов, регламентирующих режим ограниченного доступа к информации;
- формулировать технические требования стандартов в области информационной безопасности;
- разрабатывать предложения по совершенствованию системы управления информационной безопасностью;

- формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью;

владеть:

- навыками организации режима ограниченного доступа к информации доступа в соответствии с нормативными правовыми актами и нормативными методическими документами;
- развитыми навыками проведения анализа на соответствие требованиям стандартов в области информационной безопасности;
- умелыми навыками применения правовых знаний.

У обучающегося формируются следующие компетенции:

способностью использовать основы правовых знаний в различных сферах деятельности (ОК-4)

способностью использовать нормативные правовые акты в профессиональной деятельности (ОПК-5)

способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10)

способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ПК-15).

2. **Указание места дисциплины в структуре образовательной программы**

«Работа с конфиденциальной информацией» представляет дисциплину с индексом Б1.В.ДВ.10.2 базовой части учебного плана направления подготовки 10.03.01 Информационная безопасность, изучаемую на 4 курсе в 7 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 3 зачётные единицы (з.е.), 108 академических часов.

Таблица 3.1 – Объём дисциплины по видам учебных занятий

Общая трудоемкость дисциплины	108
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	54,01
лекции	36
лабораторные занятия	

практические занятия	18
экзамен	
зачет	0,1
курсовая работа (проект)	
расчетно-графическая (контрольная) работа	
Аудиторная работа (всего):	54
в том числе:	
лекции	36
лабораторные занятия	
практические занятия	18
Самостоятельная работа обучающихся (всего)	54
Контроль/экз (подготовка к экзамену)	

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

4.1 Содержание дисциплины

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

№ п/п	Раздел (тема) дисциплины	Содержание
1.	Организационные и правовые основы обеспечения безопасности конфиденциальной информации	Правовые нормы в области защиты информации. Концепция национальной безопасности Российской Федерации. Организация и функционирование системы безопасности
2.	Организационные источники и каналы утечки информации	Характеристика защитных действий. Разглашение защищаемой информации. Способы пресечения разглашения защищаемой информации. Противодействие несанкционированному доступу к информации
3.	Технические и программные средства защиты информации	Системная классификация технических средств защиты. Средства поиска закладных устройств. Средства нейтрализации технических каналов утечки информации (ТКУИ). Технические средства идентификации и установления подлинности
4.	Коммерческая тайна и порядок её определения	Защита конфиденциальных сведений. Организация работ с информацией, составляющей коммерческую тайну
5.	Организация работ с информацией, составляющей коммерческую тайну	Федеральный закон № 98-ФЗ «О коммерческой тайне». Ответственность за утрату документов. Система мер безопасности. Правила эффективной работы разрешительной системы
6.	Подбор персонала на должности, связанные с работой с информацией ограниченного доступа	Персонал организации как источник информации и один из основных каналов ее разглашения. Особенности подбора и подготовки кадров. Проверка персонала на благонадежность. Заключение контрактов и соглашений о

		секретности
7.	Организация деятельности службы безопасности объекта	Задачи службы безопасности организации. Отдел режима и охраны. Отдел защиты информации. Инженерно-техническая группа. Группа безопасности внешней деятельности
8.	Организация внутриобъектового режима	Основные задачи организация внутриобъектового режима. Организация охраны объектов на территории предприятия. Организация инженерно-технической безопасности. Организация безопасности функционирования информационных систем
9.	Требования, предъявляемые к помещениям и хранилищам, в которых ведутся закрытые работы, хранятся документы ограниченного доступа и изделия	Общие правила работы с документами в помещениях предприятия. Правила работы с конфиденциальными документами в помещениях предприятия. Требования, предъявляемые к помещениям и хранилищам, в которых ведутся закрытые работы. Требования, предъявляемые к хранящимся документам и изделиям ограниченного доступа.
10.	Организация защиты информации при приеме в организации посетителей командированных лиц и иностранных представителей	Организация приема посетителей в организации. Классификация посетителей. Угрозы информационной безопасности, исходящие от посетителей. Правила при приеме руководителем фирмы (предприятия) и руководящим составом различных категорий посетителей
11.	Организация проведения служебного расследования по фактам разглашения сотрудниками информации ограниченного доступа.	Основные понятия, связанные со служебным расследованием. Основания для проведения служебного расследования. Цели и задачи служебного расследования по фактам разглашения информации ограниченного доступа. Содержание заключения служебного расследования
12.	Охрана объектов	Цели и задачи охраны. Объекты охраны. Виды и способы охраны. Посты охраны, связь, взаимодействие с местными органами правопорядка. Использование собак и борьба с собаками нарушителя. Прием и сдача объекта под охрану. Средства и методы физической защиты объектов. Технические средства охраны и видеонаблюдения объекта. Оружие, используемое для охраны объектов. Индивидуальная защита от оружия нападения. Оборона объекта в случае нападения. Организация охраны объектов защиты в процессе их транспортировки. Противопожарная охрана
13.	Организация защиты информации при подготовке и проведению совещаний и переговоров	Основные причины, по которым информация может разглашаться на конфиденциальных совещаниях или переговорах. Документы, составляемые при подготовке конфиденциального совещания. Обязанности сотрудников службы безопасности при подготовке, проведении и окончании совещаний и переговоров
14.	Организация защиты	Источники ценных сведений в процессе выставочной

	информации при осуществлении научно-публицистической деятельности	деятельности. Обеспечение безопасности конфиденциальной информации в рекламно-выставочных материалах
15.	Защита информации при рекламной деятельности	Рекламно-выставочные материалы. Подготовка и проведение совещаний и переговоров по конфиденциальным вопросам
16.	Основные принципы организации аналитической работы служб безопасности по недопущению утечки конфиденциальной информации	Понятие информационно-аналитической работы. Основные задачи и функции информационно-аналитического подразделения службы безопасности. Принципы организации аналитической работы служб безопасности. Аналитическая работа с источниками угрозы конфиденциальной информации
17.	Подготовка лиц, ответственных за обеспечение безопасности информации	Оценка профессиональных способностей сотрудников, связанных с секретами фирмы. Организационные мероприятия по работе с персоналом, получившим доступ к конфиденциальной информации и эксплуатации систем защиты информации
18.	Содержание основных методов и работы с персоналом, обладающим конфиденциальной информацией	Анализ основных методов получения конфиденциальной информации у персонала. Особенности приема и перевода сотрудников на работу, связанную с владением конфиденциальной информацией. Текущая работа с персоналом, владеющим конфиденциальной информацией. Основные направления повышения эффективности профилактической работы с персоналом, обладающим конфиденциальной информацией

Таблица 4.2 – Содержание дисциплины и его методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости (*по неделям семестра*)	Компетенции
		лек, час	№, лаб.	№, пр.			
1	2	3	4	5	6	7	8
1.	Организационные и правовые основы обеспечения безопасности конфиденциальной информации	2		1	О-2,3,4 Д-8,9	С,Т	ОК-4, ОПК-5
2.	Организационные источники и каналы утечки информации	2		2	О-2,3,4 Д-8,9	С,Т	ОК-4, ПК-10
3.	Технические и программные средства защиты информации	2		3	О-1,2,3,4 Д-8,9	С,Т	ОПК-5, ПК-15
4.	Коммерческая тайна и порядок её определения	2		4	О-2,3,4,5 Д-2,7,8,9	С,Т	ОК-4, ПК-10

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости (*по неделям семестра*)	Компетенции
		лек, час	№, лаб.	№, пр.			
1	2	3	4	5	6	7	8
5.	Организация работ с информацией, составляющей коммерческую тайну	2		4	О-2,3,4,5 Д-2,7,8,9	С,Т	ПК-10, ПК-15
6.	Подбор персонала на должности, связанные с работой с информацией ограниченного доступа	2		4	О-2,3,4,5 Д-4,8,9	С	ОК-4
7.	Организация деятельности службы безопасности объекта	2		5	О-2,3,4,5 Д-1,4,8,9	С,Т	ОПК-5, ПК-10
8.	Организация внутриобъектового режима	2		5	О-2,3,4,5 Д-1,4,8,9	С	ОК-4, ПК-15
9.	Требования, предъявляемые к помещениям и хранилищам, в которых ведутся закрытые работы, хранятся документы ограниченного доступа и изделия	2		5	О-2,3,4,5 Д-1,4,8,9	С	ОПК-5, ПК-10
10.	Организация защиты информации при приеме в организации посетителей командированных лиц и иностранных представителей	2		6	О-2,3,4,5 Д-1,4,8,9	С,Т	ОПК-5, ПК-15
11.	Организация проведения служебного расследования по фактам разглашения сотрудниками информации ограниченного доступа.	2		6	О-2,3,4,5 Д-1,4,8,9	С,Т	ОК-4, ПК-10
12.	Охрана объектов	2		7	О-2,3,4,5 Д-1,4,8,9	С,Т	ОК-4
13.	Организация защиты информации при подготовке и проведению совещаний и переговоров	2		8	О-2,3,4,5 Д-1,6,4,8,9	С,Т	ОПК-5, ПК-10

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости (*по неделям семестра*)	Компетенции
		лек, час	№, лаб.	№, пр.			
1	2	3	4	5	6	7	8
14.	Организация защиты информации при осуществлении научно-публицистической деятельности	2		8	О-2,3,4,5 Д-1,6,4,8,9	С	ОК-4, ПК-10
15.	Защита информации при рекламной деятельности	2		8	О-2,3,4,5 Д-1,6,4,8,9	С,Т	ПК-10, ПК-15
16.	Основные принципы организации аналитической работы служб безопасности по недопущению утечки конфиденциальной информации	2		9	О-2,3,4,5 Д-1,6,4,8,9	С	ОПК-5, ПК-10
17.	Подготовка лиц, ответственных за обеспечение безопасности информации	2		9	О-2,3,4,5 Д-1,6,4,8,9	С	ОК-4, ПК-10
18.	Содержание основных методов и работы с персоналом, обладающим конфиденциальной информацией	2		9	О-2,3,4,5 Д-1,6,4,8,9	С,Т	ОПК-5, ПК-15

С – собеседование, Т – тест.

4.2 Лабораторные работы и (или) практические занятия

4.2.1 Практические работы

Таблица 4.2.1 – Практические занятия

№	Наименование лабораторной работы	Объем, час.
1.	Правовые аспекты информационной безопасности; законодательство о безопасности и защите информации; правовые методы защиты в нормативных актах других отраслей законодательства; законодательство о защите государственной тайны; законодательство о защите коммерческой тайны и других негосударственных видов тайны; законодательство о защите персональных данных; организационные документы системы защиты информации; технологические документы системы защиты информации; регламентация системы защиты информации для условий экстремальных ситуаций;	2

	рекомендательные методические указания, правила, памятки и другие пособия для персонала.	
2.	Источники, угрозы, каналы распространения и утраты конфиденциальной информации; силы, средства и условия организационной защиты информации	2
3.	Технические средства защиты информации Программные средства защиты информации	2
4.	Организация работ с информацией, составляющей коммерческую тайну; допуск и доступ к конфиденциальной информации и документам, составляющим коммерческую тайну; цель, задачи и направления классификации информационных ресурсов в предпринимательской сфере; критерии ценности, полезности и конфиденциальности информации; содержание процедуры разработки перечня ценных и конфиденциальных сведений; содержание процедуры ведения перечня ценных и конфиденциальных сведений; назначение и содержание перечня конфиденциальных документов фирмы; подбор персонала на должности, связанные с работой с информацией ограниченного доступа; классификация направлений работы с персоналом, обладающим конфиденциальной информацией; принципы, организационные формы и методика обучения и инструктирования сотрудников; принципы и направления воспитательной работы с персоналом; порядок проведения служебного расследования по фактам нарушения безопасности информации.	2
5.	Организация деятельности службы безопасности объекта; задачи службы безопасности организации. Методический подход к формированию структуры службы безопасности; организационная структура и функции службы безопасности; основные документы, регламентирующие деятельность службы безопасности объекта; особенности действий сотрудников службы безопасности в чрезвычайных ситуациях и в условиях чрезвычайного положении; способы и формы взаимодействия службы безопасности объекта с контрразведывательными и правоохранительными органами. требования, предъявляемые к помещениям и хранилищам, в которых ведутся закрытые работы, хранятся документы ограниченного доступа и изделия. общие правила работы с документами в помещениях предприятия; правила работы с конфиденциальными документами в помещениях предприятия; требования, предъявляемые к хранящимся документам и изделиям ограниченного доступа.	2

6.	Организация приема посетителей в организации; классификация посетителей; угрозы информационной безопасности, исходящие от посетителей; правила при приеме руководителем фирмы (предприятия) и руководящим составом различных категорий посетителей; организация проведения служебного расследования по фактам разглашения сотрудниками информации ограниченного доступа.	2
7.	Виды и способы охраны, посты охраны, связь, взаимодействие с местными органами правопорядка; использование собак и борьба с собаками нарушителя; прием и сдача объекта под охрану; средства и методы физической защиты объектов, технические средства охраны и видеонаблюдения объекта; оружие, используемое для охраны объектов, индивидуальная защита от оружия нападения; оборона объекта в случае нападения; организация охраны объектов защиты в процессе их транспортировки; противопожарная охрана. цели и задачи пропускного режима, организация пропускного режима; атрибутные и биометрические идентификаторы людей; порядок оформления и выдачи пропусков; контрольно-пропускные пункты людей и автотранспорта, их оборудование и организация; порядок вывоза/выноса, ввоза/вывоза материальных ценностей и документации на/с территории организации.	2
8.	Документы, составляемые при подготовке конфиденциального совещания; порядок подготовки конфиденциального совещания; обязанности сотрудников службы безопасности при подготовке, проведении и окончании совещаний и переговоров; этапы проведения конфиденциальных совещаний и переговоров: доступ участников на конфиденциальное совещание; требования к участникам конфиденциального совещания. обеспечение защиты информации при осуществлении закрытой и открытой публикации и рекламной деятельности; федеральным Законом «О рекламе». федеральный закон о СМИ; сбор информации силами предприятия, сбор информации с привлечением сторонних фирм.	2
9.	Основные принципы организации аналитической работы служб безопасности по недопущению утечки конфиденциальной информации; методы, используемые аналитическими подразделениями служб безопасности, по предупреждению утечки конфиденциальной информации. оценка профессиональных способностей сотрудников,	2

	связанных с секретами фирмы; организационные мероприятия по работе с персоналом, получившим доступ к конфиденциальной информации и эксплуатации систем защиты информации; особенности приема и перевода сотрудников на работу, связанную с владением конфиденциальной информацией; - текущая работа с персоналом, владеющим конфиденциальной информацией; основные направления повышения эффективности профилактической работы с персоналом, обладающим конфиденциальной информацией.	
Итого		18

4.3 Самостоятельная работы студентов (СРС)

Таблица 4.3 – Самостоятельная работа студентов

№ раздела (Тема)	Наименование раздела учебной дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1.	Принципы, силы, средства и условия организационной защиты информации.	4 неделя	6
2.	Особенности системы организационной защиты конфиденциальной информации.	6 неделя	6
3.	Допуск и доступ к конфиденциальной информации и документам.	8 неделя	8
4.	Организация внутриобъектового и пропускного режимов на предприятиях	12 неделя	8
5.	Организация подготовки и проведения совещаний и заседаний по конфиденциальным вопросам. Защита информации при публикаторской и рекламной деятельности	14 неделя	8
6.	Организация аналитической работы по предупреждению утечки конфиденциальной информации.	16 неделя	10
7.	Направления и методы работы с персоналом, обладающим конфиденциальной информацией.	18 неделя	8
Итого			54

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 УП и 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:

– методических рекомендаций, пособий по организации самостоятельной работы студентов;

– вопросов к экзамену, тестовых заданий;

– методических указаний к выполнению лабораторных работ, к практическим зантиям и т.д.

типографией университета:

– помощь авторам в подготовке и издании научной, учебной и методической литературы;

– удовлетворение потребности в тиражировании научной, учебной и методической литературы.

6. **Образовательные технологии**

В соответствии с требованиями ФГОС и Приказа Министерства образования и науки РФ от 05 апреля 2013 г. №301 по направлению подготовки 10.03.01 «Информационная 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. В рамках дисциплины предусмотрены встречи с экспертами и специалистами Комитета по труду и занятости населения Курской области. Удельный вес занятий, проводимых в интерактивных формах, составляет 28,8 процента от аудиторных занятий согласно УП.

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	2	3	4
1.	Принципы, силы, средства и условия организационной защиты информации.	Блицопрос Дискуссия	1
2.	Особенности системы организационной защиты конфиденциальной информации.	Блицопрос Дискуссия	1
3.	Допуск и доступ к конфиденциальной информации и документам.	Блицопрос Разбор конкретных ситуаций Дискуссия	2
4.	Организация внутриобъектового и пропускного режимов на предприятиях	Блицопрос Разбор конкретных ситуаций Дискуссия	1
5.	Организация подготовки и проведения совещаний и заседаний по конфиденциальным вопросам. Защита информации при публикаторской и рекламной деятельности	Блицопрос Разбор конкретных ситуаций Дискуссия	1
6.	Организация аналитической работы по предупреждению утечки конфиденциальной информации.	Блицопрос Разбор конкретных ситуаций Дискуссия	2
7.	Направления и методы работы с персоналом, обладающим конфиденциальной информацией.	Блицопрос Разбор конкретных ситуаций Дискуссия	2
	Итого		10

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

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

Код и содержание компетенции	Этапы* формирования компетенций и дисциплины (модуле), при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
способностью использовать основы правовых знаний в различных сферах деятельности (ОК-4)		Организационное и правовое обеспечение информационной безопасности	Организация и управление службой защиты информации; Работа с конфиденциальной

			информациией; Преддипломная практика; Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты
способностью использовать нормативные правовые акты в профессиональной деятельности (ОПК-5)	Правоведение; Патентоведение	Организационное и правовое обеспечение информационной безопасности	Организация и управление службой защиты информации; Работа с конфиденциальной информацией; Преддипломная практика; Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты
способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10)		Организационное и правовое обеспечение информационной безопасности; Учебно-исследовательская работа студентов; Проектно-технологическая практика	Организация и управление службой защиты информации; Работа с конфиденциальной информацией; Преддипломная практика; Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты
способностью организовывать технологический процесс защиты информации ограниченного доступа		Организационное и правовое обеспечение информационной безопасности;	Защита и обработка конфиденциальных документов; Организация и управление службой

в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ПК-15)		Проектно-технологическая практика	защиты информации; Работа с конфиденциальной информацией; Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты

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

Код компетенции/этап *(указывается название этапа из п 7.1)*	Показатели оценивания компетенций	Критерии шкала оценивания компетенций		
		Пороговый уровень («удовлетвори-тельно»)	Продвинутый уровень («хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
ОК-4 /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*	**Знает:** Основы правовых знаний. **Умеет:** В недостаточной форме находить правильные основы правовых знаний. **Владеет:** Основными понятиями правовых знаний	**Знает:** Основные принципы обеспечения правовых знаний. **Умеет:** Осуществлять выбор средств обеспечения правовых знаний. **Владеет:** Навыками применения правовых знаний	**Знает:** Глубокие знания в области правовых знаний в различных сферах деятельности. **Умеет:** Осуществлять рациональный выбор средств обеспечения правовых знаний. **Владеет:** Умелыми навыками применения правовых знаний

	знания, умения, навыки в типовых и нестандар-тных ситуациях			
ОПК-5/ 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 нестандар-тных ситуациях*	**Знает:** Основные понятия нормативных правовых актов. **Умеет:** Формулировать отдельные положения документов. **Владеет:** Основами нормативных правовых актов.	**Знает:** Принципы работы с нормативными правовыми актами. **Умеет:** Работать с нормативными правовыми актами. **Владеет:** Навыками применения нормативных правовых актов.	**Знает:** Полный спектр нормативных правовых актов в профессиональной деятельности. **Умеет:** Уверенно работать с нормативными правовыми актами. **Владеет:** Развитыми навыками применения нормативных правовых актов.
ПК-10/ завершающий	*1.Доля освоенных обучающимся знаний, умений навыков от общего объема ЗУН, установленных в п.1.ЗРПД* *2.Качество освоенных*	**Знает**: С пробелами основные требования стандартов в области информационной безопасности. **Умеет**: В недостаточной форме формулировать технические требования стандартов в	**Знает**: Углубленно, но с некоторыми пробелами в отдельных областях требования стандартов в области информационной безопасности. **Умеет**: В достаточной мере формулировать технические	**Знает**: Углубленно требования стандартов в области информационной безопасности. **Умеет**: Успешно формулировать технические требования стандартов в области информационной безопасности. **Владеет**:

	обучающи-мися знаний, умений, навыков *3. Умение применять знания, умения, навыки в типовых и нестандар-тных ситуациях*	области информационной безопасности. **Владеет**: Слабо владеет навыками анализа информационной безопасности объектов и систем.	требования стандартов в области информационной безопасности. **Владеет**: Навыками программирования в профессиональной сфере**.**	Развитыми навыками проведения анализа на соответствие требованиям стандартов в области информационной безопасности.
ПК-15/ завершающий способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федераци	*1.Доля освоенных обучающи мся знаний, умений навыков от общего объема ЗУН, установ-ленных в п.1.ЗРПД* *2.Качество освоенных обучающи-мися знаний, умений, навыков* *3. Умение применять знания, умения, навыки в типовых и нестандар-тных ситуациях*	**Знает:** Основные правила организации технологического процесса защиты информации ограниченного доступа. **Умеет:** Формулировать отдельные положения документов, регламентирующих режим ограниченного доступа к информации. **Владеет:** Навыками участия в организации режима ограниченного доступа к информации	**Знает:** Основные принципы организации технологического процесса защиты информации ограниченного доступа. **Умеет:** Формулировать документы регламентирующие режим ограниченного доступа к информации. **Владеет:** Организации отдельных процессов по обеспечению режима ограниченного доступа к информации	**Знает:** Глубокие знания в области организации технологического процесса защиты информации ограниченного доступа. **Умеет:** Формировать комплект документов, регламентирующих режим ограниченного доступа к информации. **Владеет:** Навыками организации режима ограниченного доступа к информации доступа в соответствии с нормативными правовыми актами и нормативными методическими документами

и, Федеральной службы по техническому и экспортному контролю				

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
				наименование	№ заданий	
1	2	3	4	5	6	7
1.	Законодательство об информационной безопасности	ОК-4,ОПК-5	Лекция, СРС, практическое занятие	Собеседование, тест, вопросы к п.р №1		Согласно табл. 7.2
2.	Организационные источники и каналы утечки информации	ОК-4, ПК-10	Лекция, СРС, практическое занятие	Собеседование, тест, вопросы к п.р №2		Согласно табл. 7.2
3.	Технические средства защиты информации	ОПК-5,ПК-15	Лекция, СРС, практическое занятие	Собеседование, тест, вопросы к п.р №3		Согласно табл. 7.2
4.	Коммерческая тайна и порядок её определения	ОК-4,ПК-10	Лекция, СРС, практическое занятие	Собеседование, тест, вопросы к п.р №4		Согласно табл. 7.2

5.	Организация внутриобъектового режима	ПК-10,ПК-15	Лекция, СРС, практическое занятие	Собесе-дование, тест, вопросы к п.р №5		Согласно табл. 7.2
6.	Организация защиты информации при приеме в организации посетителей командированных лиц и иностранных представителей	ОК-4	Лекция, СРС, практическое занятие	Собесе-дование, опросы к п.р №6		Согласно табл. 7.2
7.	Организация охраны объекта	ОПК-5,ПК-10	Лекция, СРС, практическое занятие	Собесе-дование, тест, опросы к п.р №7		Согласно табл. 7.2
8.	Организация защиты информации при подготовке и проведении совещаний и переговоров	ОК-4,ПК-15	Лекция, СРС, практическое занятие	Собесе-дование, вопросы к п.р №8		Согласно табл. 7.2
9.	Организация аналитической работы по предупреждению утечки конфиденциальной информации	ОПК-5,ПК-10	Лекция, СРС, практическое занятие	Собесе-дование, вопросы к п.р №9		Согласно табл. 7.2

Примеры типовых контрольных заданий для текущего контроля

Вопросы для собеседования

1. Нарушение целостности данных, как правило, вызвано реализацией внешних или внутренних угроз? Обоснуйте ответ.

2. Нарушение конфиденциальности данных, как правило, вызвано реализацией внешних или внутренних угроз? Обоснуйте ответ.

3. Как соотносятся между собой понятия уязвимости и угроз? Обоснуйте ответ.

4. Как соотносятся между собой понятия угроз и рисков? Обоснуйте ответ.

5. В чем заключается отличие между разглашением и утечкой информации? Обоснуйте ответ.

6. Какими способами может быть реализовано противоправное преднамеренное овладение конфиденциальной информацией? Обоснуйте ответ.

7. Каким образом может происходить бесконтрольный выход конфиденциальной информации за пределы организации? Обоснуйте ответ.

8. В чем заключается отличие между служебной и профессиональной тайной? Обоснуйте ответ.

9. Что относится к информационным активам организации, и какие информационные активы являются наиболее ценным для организаций, осуществляющих различные виды деятельности (3-4 примера)? Обоснуйте ответ.

10. Какие сведения не могут составлять коммерческую тайну? Обоснуйте ответ.

Тесты для контроля знаний

1. Должна ли предусматривать разрешительная система доступ к конфиденциальной информации должностных лиц из внешних организаций, выполняющих совместную работу с организацией где введен режим конфиденциальности?

Выберите один из 3 вариантов ответа:

1) нет, не должна

2) да, должна

3) зависит от индивидуального решения руководителя, даже если это ставит под угрозу срыва выполнение совместных работ

2. Имеют ли право на доступ к различным видам конфиденциальной информации сотрудники уполномоченных органов государственной власти (налоговая служба, служба судебных приставов, органы МВД и др.)?

Выберите один из 3 вариантов ответа:

1) нет, не имеют

2) имеют, в пределах своей компетенции

3) имеют, в пределах своей компетенции, при этом обязаны обеспечить защиту полученной информации от разглашения и неправомерного использования

3. Укажите правильный порядок введения в действие Регламента доступа к конфиденциальной информации

Укажите порядок следования всех 6 вариантов ответа:

1) Подпись (заверение) Регламента всеми членами экспертной комиссии

2) Назначение приказом директора должностных лиц в составе Экспертной комиссии по защите конфиденциальной информации.

3) Визирование Регламента всеми лицами, имеющими право давать разрешение на доступ к КИ

4) Разработка Регламента

5) Введение в действие Регламента приказом руководителя организации

6) Ознакомление с Регламентом всех сотрудников, работающих с КИ

4. Кто входит в круг лиц, имеющих право давать разрешение на допуск и доступ к конфиденциальной информации? Ответов несколько.

Выберите несколько из 5 вариантов ответа:

1) Руководитель организации

2) Любой сотрудник, имеющий доступ к КИ

3) Руководитель структурного подразделения всем сотрудникам

4) Руководитель структурного подразделения в пределах своей компетенции

5) Заместитель руководителя в пределах своей сферы деятельности

5. В каком виде выдается разрешение на работу с конфиденциальными документами?

Выберите один из 3 вариантов ответа:

1) в устной форме

2) в виде письма по почте

3) в виде резолюции

6. В случае организации системы доступа к КИ с сотрудниками из других организаций какие документы будут с ними подписаны?

Выберите один из 4 вариантов ответа:

1) договор и обязательство о неразглашении

2) только договор

3) только обязательство

4) все зависит от пожеланий руководителя организации

7. Кто такой контрагент в рамках реализации работ с КИ со сторонней организацией?

Выберите один из 3 вариантов ответа:

1) это постороннее для организации лицо

2) это адресат

3) это сторона гражданско-правового договора

8. Обязан ли контрагент сообщить обладателю конфиденциальной информации о допущенном им же (контрагентом) факте разглашения КИ?

Выберите один из 2 вариантов ответа:

1) да

2) нет

9. Кому сотрудник сообщит о попытке посторонних лиц получить от него КИ и кому сотрудник в случае увольнения сдаст все носители КИ?

Выберите один из 4 вариантов ответа:

1) сотруднику службы конфиденциального делопроизводства и руководителю организации

2) никому ничего не должен сообщать и передавать

3) руководителю организации и сотруднику службы конфиденциального делопроизводства

4) в вариантах не перечислено этих лиц

10. Что относится к специальным (особым) категориям персональных данных?

Выберите один из 3 вариантов ответа:

1) состояние здоровья, политические взгляды, национальность

2) фамилия, имя, отчество

3) биометрические данные

Полностью оценочные средства представлены в учебно-методическом комплексе дисциплины.

Типовые задания для промежуточной аттестации

Проверяемыми на промежуточной аттестации элементами содержания являются темы дисциплины, указанные в разделе 4 настоящей программы. Все темы дисциплины отражены в КИМ в равных долях (%).

Для проверки *знаний* используются вопросы и задания в закрытой форме (с выбором одного или нескольких правильных ответов).

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

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

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

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, 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
1	2	3	4	5
Практическое занятие №1 Порядок засекречивания и рассекречивания сведений, документов и продукции	2	Выполнил, но «не защитил»	4	Выполнил, и «защитил»
Практическое занятие №2 Порядок допуска к секретной (конфиденциальной) информации	2	Выполнил, но «не защитил»	4	Выполнил, и «защитил»
Практическое занятие №3 Порядок допуска к секретной (конфиденциальной) информации	2	Выполнил, но «не защитил»	4	Выполнил, и «защитил»
Практическое занятие №4 Допуск и доступ к конфиденциальной информации и документам, составляющим коммерческую тайну	2	Выполнил, но «не защитил»	4	Выполнил, и «защитил»
Практическое занятие №5 Организационные источники и каналы утечки информации. Силы, средства и условия организационной защиты информации	2	Выполнил, но «не защитил»	4	Выполнил, и «защитил»
Практическое занятие №6	2	Выполнил, но «не защитил»	4	Выполнил, и «защитил»
Практическое занятие №7 Обеспечение режима секретности при деятельности объекта	2	Выполнил, но «не защитил»	4	Выполнил, и «защитил»
Практическое занятие №8 Организация работ с информацией, составляющей коммерческую тайну	2	Выполнил, но «не защитил»	4	Выполнил, и «защитил»
Практическое занятие №9 Допуск и доступ к конфиденциальной информации и документам, составляющим коммерческую тайну	2	Выполнил, но «не защитил»	4	Выполнил, и «защитил»
Защита реферата	2	Выполнил,	4	Выполнил,

		но «не защитил»		и «защитил»
СРС	4		8	
Итого	24		48	
Посещаемость	0		16	
Зачет	0		36	
Итого	24		100	

Итоговый контроль – в форме компьютерного теста. Студенту предлагается 20 вопросов по различным темам курса из 5 категорий сложности. Вопросы 1-й категории сложности оцениваются в 1 условный балл, 2-й – в 2 условных балла, и т. д. В каждом вопросе один правильный ответ. Полученную итоговую сумму условных баллов (максимум 60) переводят в баллы на зачете/экзамене (максимум 36) путём умножения на 0.6 и округления до целого значения.

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

8.1 Основная учебная литература

1) Запечников С.В. Информационная безопасность открытых систем [Текст] : учебник. Т.1: Угрозы, уязвимости, атаки и подходы к защите. - М.: Горячая линия - Телеком, 2006. - 536 с.

2) Мельников В. П. Информационная безопасность и защита информации [Текст] : учебное пособие / В. П. Мельников, С. А. Клейменов, А. М. Петраков. - М.: Академия, 2006. - 336 с.

3) Казанцева С. Я. Правовое обеспечение информационной безопасности [Текст] : учебное пособие. - 3-е изд., стер. - М.: Академия, 2008. - 240 с.

4) Мельников В.П. Информационная безопасность и защита информации [Текст] : учебное пособие. - М.: Изд. центр “Академия”, 2006. – 336 с.

8.2 Дополнительная учебная литература

1) Грибулин Н.В. Комплексная система защиты информации на предприятии [Текст] М.: Изд. центр “Академия”, 2009. – 416 с.

2) Ишейнов В.Я.,Мецатуанян М.В. Защита конфиденциальной информации [Текст] М.: Форум, 2013. – 256с.

3) Методика информационной безопасности. Под рук. Уфимцева Ю.С. [Текст] М.: ЭКЗАМЕН, 2004.

4) Технические средства и методы защиты информации. Под ред. Зайцева А.П. [Текст] М.: Горячая линия- Телеком, 2009.

5) Аверченков В.И., М.Ю. Рытов Организационная защита информации [Текст] Учебник – Брянск.: БГТУ.,2005.

6) Корнеев И.К., Степанов Е.А. Защита информации в офисе [Текст] М.: Проспект, 2008.

7) Бабенко Л.К., Кухаренко А.П., Макаревич О.Б. и др. Методическое пособие по курсу «Защита информации в предпринимательской деятельности» [Текст] /Таганрог: Изд-во ТРТУ, 2000.

8) Волокитин А. В., Маношкин А. П., Солдатенков А. В. и др. Информационная безопасность государственных организаций и коммерческих фирм: Справочное пособие [Текст] /Под ред. Реймана Л.Д. – М.: ФИОРД-ИНФО, 2002.

9) Дворянкин С.В. , Минаев В.А. и др. Правовое обеспечение информационной безопасности [Текст] / М.: Проспект, 2008.

8.3 Перечень методических указаний

1. Работа с конфиденциальной информацией [Электронный ресурс]: методические указания по выполнению практических работ / Юго-Западный государственный университет; сост.: О.А. Демченко. - Электрон. текстовые дан. - Курск : ЮЗГУ, 2017. - 51 с.

2. Работа с конфиденциальной информацией [Электронный ресурс]: Методические указания по выполнению самостоятельных работ / Юго-Западный государственный университет; сост.: О.А. Демченко. - Электрон. текстовые дан. - Курск : ЮЗГУ, 2017. - 29 с.

3. Работа с конфиденциальной информацией (Методические указания по выполнению практических заданий и самостоятельной работы) / Юго-Западный государственный университет; сост.: О.А. Демченко, В.В. Карасовский. - Электрон. текстовые дан. - Курск : ЮЗГУ, 2017. - 32 с.

8.4 Другие учебно-методические материалы

9. Перечень ресурсов информационно-телекаммуникационной сети «Интернет», необходимых для освоения дисциплины

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

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

6. Википедия. Свободная энциклопедия [официальный сайт]. Режим доступа: https://ru.wikipedia.org/

10. **Методические указания для обучающихся по освоению дисциплины**

Основными видами аудиторной работы студента при изучении дисциплины «Работа с конфиденциальной информацией» 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 лабораторным работам, а также по результатам докладов.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Работа с конфиденциальной информацией»: 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 с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины 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

12. **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	

Приложение А Вопросы к зачету

1. Организационные методы обеспечения безопасности конфиденциальной информации.
2. Требования к построению систем безопасности предприятия и учреждения.
3. Правовые основы организационного обеспечения безопасности конфиденциальной информации.
4. Характеристика защитных действий от утечки информации.
5. Способы пресечения разглашения защищаемой информации.
6. Противодействие несанкционированному доступу к конфиденциальной информации.
7. Технические средства защиты конфиденциальной информации.
8. Программные средства защиты конфиденциальной информации.
9. Организация работ с информацией, составляющей коммерческую тайну.
10. Порядок допуска к работам с информацией, составляющей коммерческую тайну.
11. Порядок подбора персонала на должности, связанные с работой с информацией ограниченного доступа.
12. Порядок заключения контрактов и соглашений о неразглашении конфиденциальной информации.
13. Задачи службы безопасности организации.
14. Организационная структура и функции службы безопасности.
15. Структурные подразделения службы безопасности.
16. Основные задачи организации внутриобъектового режима.
17. Организация охраны объектов на территории предприятия.
18. Организация инженерно-технической безопасности предприятия.
19. Организация безопасности функционирования информационных систем.
20. Назначение и основные задачи контрольно-пропускного пункта объекта.
21. Защита периметра территории зданий и открытых площадок с помощью технических средств охраны.
22. Защита помещений объекта с помощью технических средств охраны.
23. Системы контроля и управления доступом к конфиденциальной информации.
24. Системы охранного телевидения и оповещения.
25. Организация приема посетителей в организации. Классификация посетителей.
26. Угрозы информационной безопасности, исходящие от посетителей.
27. Правила при приеме руководителем фирмы (предприятия) и руководящим составом различных категорий посетителей.

28. Работа с иностранными представителями.
29. Назначение и порядок проведения проверки наличия документов, дел и носителей конфиденциальной информации.
30. Организация служебного расследования по фактам разглашения сотрудниками конфиденциальной информации.
31. Организация охраны объектов.
32. Организация пропускного режима.
33. Основные факторы, приводящие к разглашению конфиденциальной информации на совещании и переговорах.
34. Этапы проведения конфиденциальных совещаний и переговоров.
35. Документы, составляемые при подготовке конфиденциального совещания и порядок подготовки и проведения конфиденциального совещания.
36. Основные обязанности сотрудников службы безопасности при подготовке и проведении совещаний и переговоров.
37. Порядок доступа участников на конфиденциальные совещания.
38. Организация защиты информации при осуществлении научно-публицистической деятельности.
39. Организации защиты конфиденциальной информации при рекламной деятельности.
40. Понятие информационно-аналитической работы.
41. Основные задачи и функции информационно-аналитического подразделения службы безопасности.
42. Аналитическая работа с источниками угрозы конфиденциальной информации.
43. Выбор и подготовка персонала к работе, связанной с секретами фирмы.
44. Обучение персонала правилам защиты конфиденциальной информации.
45. Организационные мероприятия по работе с персоналом, получившим доступ к конфиденциальной информации.
46. Анализ нарушений режима конфиденциальности информации.
47. Меры предупреждения обстоятельств организационно-управленческого, воспитательного и правового характера.
48. Изучение личности нарушителя режима конфиденциальности

Приложение Б Темы рефератов

1. Понятие, проблемы и структура экономической безопасность предпринимательской деятельности (на примере фирм различных типов).
2. Классификация информационных ресурсов ограниченного доступа к ним персонала фирмы, характеристика каждой группы.
3. Информационная безопасность, история формирования.
4. Концепция информационной безопасности.
5. Основы экономической безопасности предпринимательской деятельности.
6. Анализ законодательных актов о защите информационных ресурсов ограниченного доступа.
7. Соотношение понятий: информационные ресурсы, информационные системы и информационная безопасность.
8. Информационная безопасность (по материалам зарубежных источников и литературы).
9. Правовые основы защиты конфиденциальной информации.
10. Экономические основы защиты конфиденциальной информации.
11. Организационные основы защиты конфиденциальной информации.
12. Структура, содержание и методика составления перечня сведений, составляющих предпринимательскую тайну.
13. Построение и функционирование защищенного документооборота.
14. Анализ инструкции по обработке и хранению конфиденциальных документов.
15. Направления и методы защиты документов на бумажных носителях.
16. Направления и методы защиты машиночитаемых документов.
17. Направления и методы защиты электронных документов.
18. Архивное хранение конфиденциальных документов.
19. Направления и методы защиты аудио и визуальных документов.
20. Виды и назначение технических средств защиты информации в помещениях, используемых для ведения переговоров и совещаний.
21. Организационное обеспечение защиты информации, обрабатываемой средствами вычислительной и организационной техники.
22. Соотношение источников, каналов распространения и каналов утечки информации.
23. Анализ опыта защиты информации в зарубежных странах.
24. Анализ конкретной автоматизированной системы, предназначенной для обработки и хранения информации о конфиденциальных документах фирмы.
25. Основы технологии обработки и хранения конфиденциальных документов.

26. Назначение, виды, структура и технология функционирования системы защиты информации.

27. Направления экономического анализа системы защиты информации.

28. Поведение персонала и охрана фирмы в экстремальных ситуациях различных типов.

29. Направления и методы защиты профессиональной тайны.

30. Направления и методы защиты служебной тайны.

31. Направления и методы защиты персональных данных о гражданах.

32. Методы защиты личной и семейной тайны.

33. Защита секретов в дореволюционной России.

34. Проблемы управления персоналом и защиты информации в предпринимательской деятельности.

35. Порядок подбора персонала для работы с конфиденциальной информацией.

36. Тестирование и проведение собеседования с претендентами на должность, связанную с секретами фирмы.

37. Назначение, структура и методика построения разрешительной системы доступа персонала к секретам фирмы.

38. Порядок подготовки и проведения переговоров и совещаний по конфиденциальным вопросам.

39. Классификация посетителей фирмы, характеристика каждой группы.

40. Защита информации в рекламной и выставочной деятельности.

41. Анализ функций секретаря-референта небольшой фирмы в области защиты информации.

42. Направления защиты компьютеров и локальных сетей от несанкционированного доступа к информации.

43. Составление библиографии по проблемам экономической безопасности, защиты предпринимательской тайны и конфиденциальной информации (российская и зарубежная литература).

44. Процессуальные проблемы защиты информации в зарубежных странах.

45. Анализ существующих схем доступа персонала в помещения фирмы.

46. Аналитический обзор опыта зарубежных стран в регламентации управления персоналом, обладающим конфиденциальной информацией.

47. Аналитический обзор российского и зарубежного исторического опыта в предотвращении утраты ценной информации по вине сотрудников.

48. Анализ существующих правил поведения персонала и охраны фирмы в экстремальных ситуациях различного типа.

49. Проблемы управления персоналом и защиты информации в предпринимательской деятельности (теоретический очерк).

50. Психологические и профессиональные особенности личности человека, владеющего тайной, мотивации мышления и поведения.

51. Цели, задачи, стадии и методы работы с персоналом, обладающим конфиденциальной информацией.

52. Технологическая схема приема (перевода) сотрудников на работу, связанную с владением конфиденциальной информацией.

53. Классификация персонала фирмы и окружающих фирму людей по степени их осведомленности в тайнах фирмы, анализ каждой классификационной группы.

54. Классификация экстремальных ситуаций, угрожающих персоналу фирмы в рабочее и нерабочее время, анализ выделенных классификационных групп и методов локализации опасности.

55. Порядок и методика проведения служебного расследования по фактам нарушения правил защиты секретов фирмы.

56. Факторы, предпосылки и условия применения различных форм морального и материального стимулирования ответственного отношения сотрудников к обеспечению информационной безопасности фирмы.

57. Место и роль психологического климата в коллективе при проведении воспитательной работы в коллективе фирмы.

58. Классификация противоправных действий персонала фирмы с конфиденциальной информацией.

59. Принципы построения, организация и совершенствование пропускного режима на фирме, методика идентификации различных категорий сотрудников и посетителей.

60. Анализ функциональной и информационной взаимосвязи службы безопасности и службы персонала фирмы.