МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Проректор по учебной работе

Документ подписан электронной подписью
Сертификат: 1c6cfa0a-52a6-4f49-aef0-5584d3fd4820
Владелец: Троян Павел Ефимович
Действителен: с 19.01.2016 по 16.09.2019

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Системы защиты информации в ведущих зарубежных странах

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки (специальность): **10.03.01 Информационная безопасность**
Направленность (профиль): **Организация и технология защиты информации**
Форма обучения: **очная**
Факультет: **РТФ, Радиотехнический факультет**
Кафедра: **РЗИ, Кафедра радиоэлектроники и защиты информации**
Курс: **4**
Семестр: **7**
Учебный план набора 2013 года

Распределение рабочего времени

№	Виды учебной деятельности	7 семестр	Всего	Единицы
1	Лекции	24	24	часов
2	Практические занятия	36	36	часов
3	Всего аудиторных занятий	60	60	часов
4	Из них в интерактивной форме	20	20	часов
5	Самостоятельная работа	48	48	часов
6	Всего (без экзамена)	108	108	часов
7	Общая трудоемкость	108	108	часов
		3.0	3.0	З.Е

Зачет: 7 семестр

Томск 2017

Согласована на портале № 19215

Рассмотрена и одобрена на заседании кафедры
протокол № 4 от «24» 1 2017 г.

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.03.01 Информационная безопасность, утвержденного 01 декабря 2016 года, рассмотрена и утверждена на заседании кафедры «___» _____ 20__ года, протокол №_____.

Разработчик:

доцент каф. РЗИ _____ А. П. Кшнянкин

Заведующий обеспечивающей каф.
РЗИ _____ А. С. Задорин

Рабочая программа согласована с факультетом, профилирующей и выпускающей кафедрами направления подготовки (специальности).

Декан РТФ _____ К. Ю. Попова

Заведующий выпускающей каф.
РЗИ _____ А. С. Задорин

Эксперт:

ведущий инженер каф. РЗИ _____ Ю. В. Зеленецкая

Согласована на портале № 19215

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Формирование у студентов устойчивых основ знаний систем защиты ведущих зарубежных стран, приобретения при этом необходимых умений и навыков.

1.2. Задачи дисциплины

- • изучение проблем защиты информации в мировой практике;
- • изучение особенностей современных систем защиты информации в ведущих зарубежных странах, а именно: США, страны Евросоюза, КНР, Япония;
- • изучение проблем информационного противоборства в системе политических отношений современного информационного общества;
- • изучение методов добывания информации;
- • изучение международных стандартов информационной безопасности.
-

2. Место дисциплины в структуре ОПОП

Дисциплина «Системы защиты информации в ведущих зарубежных странах» (Б1.В.ОД.9) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Организационное и правовое обеспечение информационной безопасности, Техническая защита информации.

Последующими дисциплинами являются: Комплексные системы защиты информации на предприятии, Организация и управление службой защиты информации на предприятии.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ОК-5 способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики;
- ПК-9 способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;

В результате изучения дисциплины студент должен:

- **знать** • основные требования к безопасности информационных систем в США, странах Евросоюза, Японии и Китае. • историю создания систем защиты информации в США, странах Евросоюза, Японии и Китае. • порядок контроля и координации деятельности органов защиты информации в США, странах Евросоюза, Японии и Китае, особенности защиты государственной тайны в этих странах. • организацию информационно-психологического обеспечения современных военных конфликтов в США. • основные направления Национального плана по защите информационных систем в США. • характеристики основных положений Европейской директивы по защите данных. • особенности международного сотрудничества в области информационной безопасности в мире. • характеристики основных объектов и средств физической защиты, применяемых ведущими зарубежными странами в системе защиты территорий и помещений. основные международные стандарты информационной безопасности
- **уметь** • классифицировать различные объекты и средства, определять требования к их защите на объектах информатизации ведущих зарубежных стран в том числе и от утечки по техническим каналам; • проводить анализ защищённости объектов и определять класс защиты информации по международным стандартам; • формулировать рекомендации по увеличению уровня защищённости российских объектов информатизации на основе опыта защиты информации в ведущих за рубежных странах.
- **владеть** • навыками использования систем защиты информации в ведущих зарубежных странах при обеспечении информационной безопасности предприятий.

Согласована на портале № 19215

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 3.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		7 семестр
Аудиторные занятия (всего)	60	60
Лекции	24	24
Практические занятия	36	36
Из них в интерактивной форме	20	20
Самостоятельная работа (всего)	48	48
Проработка лекционного материала	11	11
Подготовка к практическим занятиям, семинарам	37	37
Всего (без экзамена)	108	108
Общая трудоемкость ч	108	108
Зачетные Единицы	3.0	3.0

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

Названия разделов дисциплины	Лекции	Практические занятия	Самостоятельная работа	Всего часов (без экзамена)	Формируемые компетенции
7 семестр					
1 Введение	2	0	1	3	ОК-5, ПК-9
2 История развитие систем защиты информации в ведущих зарубежных странах.	2	4	5	11	ОК-5, ПК-9
3 Организация защиты информации в США.	2	4	5	11	ОК-5, ПК-9
4 Организация защиты информации в Германии.	2	4	5	11	ОК-5, ПК-9
5 Организация защиты информации в Великобритании.	2	4	5	11	ОК-5, ПК-9
6 Организация защиты информации во Франции.	2	4	5	11	ОК-5, ПК-9
7 Организация защиты информации в Японии.	2	4	5	11	ОК-5, ПК-9
8 Организация защиты информации в КНР.	2	4	5	11	ОК-5, ПК-9

Согласована на портале № 19215

9 Стандарты информационной безопасности.	4	4	6	14	ОК-5, ПК-9
10 Международное сотрудничество в области защиты информации.	2	2	3	7	ОК-5, ПК-9
11 Информационное противоборство в системе международных отношений.	2	2	3	7	ОК-5, ПК-9
Итого за семестр	24	36	48	108	
Итого	24	36	48	108	

5.2. Содержание разделов дисциплины (по лекциям)

Содержание разделов дисциплин (по лекциям) приведено в таблице 5.2.

Таблица 5.2 - Содержание разделов дисциплин (по лекциям)

Названия разделов	Содержание разделов дисциплины по лекциям	Трудоемкость, ч	Формируемые компетенции
7 семестр			
1 Введение	Предмет и задачи курса. Взаимосвязь курса с другими дисциплинами. Разделы и темы, их распределение по видам аудиторных занятий. Формы проведения семинарских занятий. Состав самостоятельной работы студентов по изучению дисциплины. Анализ нормативных источников, научной и учебной литературы.	2	ОК-5, ПК-9
	Итого	2	
2 История развитие систем защиты информации в ведущих зарубежных странах.	Особенности опыта организации защиты информации на Древнем Востоке. История основных направлений, принципов и методов защиты информации в средневековой Европе. Создание первых европейских государственных секретных служб (на примере Англии, Франции, Германии). Опыт криптографической защиты информации в странах Западной Европы. Методы защиты коммерческих сведений. Формирование особенностей политики защиты государственных секретов и коммерческой тайны в странах Западной Европы, США и Японии в XVIII – XX в.в. Разведка и контрразведка как элементы политики обеспечения безопасности государств. Промышленный шпионаж: его значение для формирования систем защиты информации. Особенности государственной политики по отношению к промышленному шпионажу в	2	ОК-5, ПК-9

Согласована на портале № 19215

	национальных и межгосударственных рамках. Формирование авторского и патентного права. Особенности формирования современных систем защиты информации в ведущих зарубежных странах в XXI в.		
	Итого	2	
3 Организация защиты информации в США.	Государственная политика в области защиты информации. Организация защиты информации по национальной безопасности (государственных секретов). Состав и основные функции органов, осуществляющих защиту информации по национальной безопасности. Особенности организации защиты информации в промышленности. Защита секретной информации, используемой в международных программах. Доступ к правительственной информации. Порядок предоставления доступа к информации лицам, не являющимся гражданами США. Организация защиты коммерческой тайны. Классификация информации, составляющей коммерческую тайну. Доступ к информации, принадлежащей частным лицам. Организация контроля надежности функционирования системы защиты коммерческой тайны фирмы. Требования к персоналу. Особенности подбора, проверки, подготовки, текущей работы с персоналом, допущенным к информации, составляющей коммерческую тайну фирмы.	2	ОК-5, ПК-9
	Итого	2	
4 Организация защиты информации в Германии.	Государственная политика в области защиты информации. Организация системы специальных служб в области защиты информации. Парламентско-правительственный контроль за деятельностью специальных служб. Состав, структура и основные направления деятельности служб безопасности. Общественные организации по борьбе с экономическим шпионажем и преступностью. Взаимодействие системы специальных служб и правоохранительных органов с частными промышленными и коммерческими службами безопасности. Особенности подбора, проверки, профессиональной подготовки, текущей работы с персоналом,	2	ОК-5, ПК-9

Согласована на портале № 19215

	допущенным к защищаемой информации. Особенности защиты информации в банковской сфере. Правовые основы защиты информации. Государственная тайна и доступ к правительственной, парламентской и судебной информации. Правовая защита служебной, налоговой тайны, тайны судебного разбирательства, тайны почтовых и телесообщений, коммерческой и производственной тайны. Организация доступа к информации, принадлежащей частным лицам.		
	Итого	2	
5 Организация защиты информации в Великобритании.	Государственная политика в области защиты информации. Организация системы специальных служб и их основные функции в области защиты информации. Функции специальных подразделений министерства торговли и промышленности по предупреждению коммерческих преступлений. Особенности подбора, проверки, профессиональной подготовки, текущей работы с персоналом, допущенным к защищаемой информации. Содержание программы обеспечения безопасности предприятия. Особенности защиты информации и предупреждение компьютерных преступлений в банковской сфере. Классификация защищаемой информации. Правовые основы защиты информации. Государственная тайна и организация доступа к правительственной информации. Правовая защита тайны корреспонденции. Коммерческая тайна и доступ к информации, принадлежащей частным лицам.	2	ОК-5, ПК-9
	Итого	2	
6 Организация защиты информации во Франции.	Государственная политика в области защиты информации. Организация системы специальных служб и их основные функции в области защиты информации. Службы безопасности в промышленно-торговых фирмах и финансовых учреждениях (банках, страховых компаниях, инвестиционных фирмах). Службы безопасности в фирмах, выполняющих государственные заказы в сфере оборонной промышленности, космических и ядерных исследований, новых видов вооружений, средств свя-	2	ОК-5, ПК-9

Согласована на портале № 19215

	зи и транспорта. Особенности подбора, проверки, профессиональной подготовки, текущей работы с персоналом, допущенным к защищаемой информации. Особенности защиты информации в банковской сфере. Правовые основы защиты информации. Государственная тайна и организация доступа к правительственной информации, парламентским заседаниям, публикация парламентских документов. Правовая защита служебной, профессиональной тайны, тайны корреспонденции. Коммерческая тайна и организация доступа к информации, принадлежащей частным предприятиям.		
	Итого	2	
7 Организация защиты информации в Японии.	Государственная политика в области защиты информации. Организация системы специальных служб и их функции в области защиты информации. Общественные организации, оказывающие помощь органам полиции в сфере защиты экономической информации (территориальные советы по предупреждению преступности, общества содействия полиции, пункты связи по предупреждению преступности). Службы безопасности отдельных организаций. Подразделения внутреннего самоконтроля отдельных организаций и их функции в сфере защиты информации. Особенности подбора, проверки, профессиональной подготовки, текущей работы с персоналом, допущенным к защищаемой информации. Принцип корпоративной защиты и обеспечения безопасности объекта. Защита информации в процессе взаимодействия фирм с иностранными партнерами. Правовые основы защиты информации.	2	ОК-5, ПК-9
	Итого	2	
8 Организация защиты информации в КНР.	Представление об информационном противоборстве в Китае. Государственная политика в области защиты информации. Организация системы специальных служб и их функции в области защиты информации. Организационная структура спецслужб Китая. Законодательство в сфере информационной безопасности в Китае. «Великая стена»	2	ОК-5, ПК-9

Согласована на портале № 19215

	информационной безопасности Китае.		
	Итого	2	
9 Стандарты информационной безопасности.	Предпосылки создания стандартов информационной безопасности. Стандарт «Критерии оценки надежности компьютерных систем» (Оранжевая книга). Гармонизированные критерии европейских стран. Германский стандарт BSI. Британский стандарт BS 7799. Международный стандарт ISO 17799. Международный стандарт ISO 15408 «Общие критерий». Стандарт COBIT.	4	ОК-5, ПК-9
	Итого	4	
10 Международное сотрудничество в области защиты информации.	Научно-техническое сотрудничество с зарубежными партнерами. Организация защиты информации в процессе проведения международных конференций, симпозиумов, обмена специалистами и др. Регламентация процедур обеспечения защиты информации в ходе посещения представителями зарубежных фирм охраняемых объектов. Порядок предоставления защищаемой информации другим странам. Международный опыт защиты информации в процессе банковской деятельности. Международный опыт стандартизации в области защиты информации. Международная защита интеллектуальной собственности. Международные договоры и иные международно-правовые документы (Всеобщая декларация прав человека, Международный пакт о гражданских и политических правах, Договор об образовании Европейского экономического сообщества и др.) о защите информации, предупреждении недобросовестной конкуренции в процессе международного предпринимательства, предупреждении компьютерных преступлений.	2	ОК-5, ПК-9
	Итого	2	
11 Информационное противоборство в системе международных отношений.	Современная картина международных отношений в мире. Основы информационно-психологического воздействия. Типы информационного оружия.	2	ОК-5, ПК-9
	Итого	2	
Итого за семестр		24	

Согласована на портале № 19215

5.3. Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами

Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами представлены в таблице 5.3.

Таблица 5.3 - Разделы дисциплины и междисциплинарные связи

Наименование дисциплин	№ разделов данной дисциплины, для которых необходимо изучение обеспечивающих и обеспечиваемых дисциплин										
	1	2	3	4	5	6	7	8	9	10	11
Предшествующие дисциплины											
1 Организационное и правовое обеспечение информационной безопасности	+	+	+	+	+	+	+		+	+	+
2 Техническая защита информации		+	+	+	+	+	+	+	+	+	+
Последующие дисциплины											
1 Комплексные системы защиты информации на предприятии			+	+	+	+	+	+	+	+	+
2 Организация и управление службой защиты информации на предприятии	+	+	+	+	+	+	+	+	+	+	+

5.4. Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий представлено в таблице 5.4

Таблица 5.4 – Соответствие компетенций и видов занятий, формируемых при изучении дисциплины

Компетенции	Виды занятий			Формы контроля
	Лекции	Практические занятия	Самостоятельная работа	
ОК-5	+	+	+	Конспект самоподготовки, Опрос на занятиях, Зачет, Выступление (доклад) на занятии
ПК-9	+	+	+	Конспект самоподготовки, Опрос на занятиях, Зачет, Выступление (доклад) на занятии

6. Интерактивные методы и формы организации обучения

Технологии интерактивного обучения при разных формах занятий в часах приведены в таблице 6.1

Согласована на портале № 19215

Таблица 6.1 – Технологии интерактивного обучения при разных формах занятий в часах

Методы	Интерактивные практические занятия	Интерактивные лекции	Всего
7 семестр			
Мозговой штурм	6	2	8
Решение ситуационных задач	3	4	7
Презентации с использованием слайдов с обсуждением	3	2	5
Итого за семестр:	12	8	20
Итого	12	8	20

7. Лабораторные работы

Не предусмотрено РУП

8. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 8.1.

Таблица 8. 1 – Наименование практических занятий (семинаров)

Названия разделов	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
7 семестр			
2 История развитие систем защиты информации в ведущих зарубежных странах.	Особенности опыта организации защиты информации на Древнем Востоке. История основных направлений, принципов и методов защиты информации в средневековой Европе. Создание первых европейских государственных секретных служб (на примере Англии, Франции, Германии). Опыт криптографической защиты информации в странах Западной Европы. Особенности формирования современных систем защиты информации в ведущих зарубежных странах в XX в.	4	ОК-5, ПК-9
	Итого	4	
3 Организация защиты информации в США.	Государственная политика в области защиты информации. Организация защиты информации по национальной безопасности (государственных секретов). Особенности организации защиты информации в промышленности. Защита секретной информации, используемой в международных программах. Доступ к правительственной информации. Порядок предоставления доступа к информации лицам, не являющимся гражданами США. Организация защиты коммерческой тайны.	4	ОК-5, ПК-9

Согласована на портале № 19215

	Классификация информации, составляющей коммерческую тайну. Доступ к информации, принадлежащей частным лицам. Организация контроля надежности функционирования системы защиты коммерческой тайны фирмы.		
	Итого	4	
4 Организация защиты информации в Германии.	Государственная политика в области защиты информации. Организация системы специальных служб в области защиты информации. Парламентско-правительственный контроль за деятельностью специальных служб. Особенности защиты информации в банковской сфере. Правовые основы защиты информации. Государственная тайна и доступ к правительственной, парламентской и судебной информации. Правовая защита служебной, налоговой тайны, тайны судебного разбирательства, тайны почтовых и телесообщений, коммерческой и производственной тайны.	4	ОК-5, ПК-9
	Итого	4	
5 Организация защиты информации в Великобритании.	Государственная политика в области защиты информации. Организация системы специальных служб и их основные функции в области защиты информации. Содержание программы обеспечения безопасности предприятия. Особенности защиты информации и предупреждение компьютерных преступлений в банковской сфере. Классификация защищаемой информации. Правовые основы защиты информации. Государственная тайна и организация доступа к правительственной информации. Правовая защита тайны корреспонденции. Коммерческая тайна и доступ к информации, принадлежащей частным лицам.	4	ОК-5, ПК-9
	Итого	4	
6 Организация защиты информации во Франции.	Государственная политика в области защиты информации. Организация системы специальных служб и их основные функции в области защиты информации. Особенности защиты информации в банковской сфере. Правовые основы защиты информации. Государственная тайна и организация доступа к правительственной информации, парламентским заседаниям, публикация	4	ОК-5, ПК-9

Согласована на портале № 19215

	парламентских документов. Правовая защита служебной, профессиональной тайны, тайны корреспонденции. Коммерческая тайна и организация доступа к информации, принадлежащей частным предприятиям.		
	Итого	4	
7 Организация защиты информации в Японии.	Государственная политика в области защиты информации. Организация системы специальных служб и их функции в области защиты информации. Общественные организации, оказывающие помощь органам полиции в сфере защиты экономической информации.	4	ОК-5, ПК-9
	Итого	4	
8 Организация защиты информации в КНР.	Представление об информационном противоборстве в Китае. Государственная политика в области защиты информации. Законодательство в сфере информационной безопасности в Китае. «Великая стена» информационной безопасности Китае.	4	ОК-5, ПК-9
	Итого	4	
9 Стандарты информационной безопасности.	Стандарт «Критерии оценки надежности компьютерных систем» (Оранжевая книга). Гармонизированные критерии европейских стран. Германский стандарт BSI. Британский стандарт BS 7799. Международный стандарт ISO 17799. Международный стандарт ISO 15408 «Общие критерий». Стандарт COBIT.	4	ОК-5, ПК-9
	Итого	4	
10 Международное сотрудничество в области защиты информации.	Научно-техническое сотрудничество с зарубежными партнерами. Организация защиты информации в процессе проведения международных конференций, симпозиумов, обмена специалистами и др.	2	ОК-5, ПК-9
	Итого	2	
11 Информационное противоборство в системе международных отношений.	Основы информационно-психологического воздействия. Типы информационного оружия.	2	ОК-5, ПК-9
	Итого	2	
Итого за семестр		36	

9. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 9.1.

Согласована на портале № 19215

Таблица 9.1 - Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
7 семестр				
1 Введение	Проработка лекционного материала	1	ОК-5, ПК-9	Выступление (доклад) на занятии, Зачет, Конспект самоподготовки, Опрос на занятиях
	Итого	1		
2 История развитие систем защиты информации в ведущих зарубежных странах.	Подготовка к практическим занятиям, семинарам	4	ОК-5, ПК-9	Выступление (доклад) на занятии, Зачет, Конспект самоподготовки, Опрос на занятиях
	Проработка лекционного материала	1		
	Итого	5		
3 Организация защиты информации в США.	Подготовка к практическим занятиям, семинарам	4	ОК-5, ПК-9	Выступление (доклад) на занятии, Зачет, Конспект самоподготовки, Опрос на занятиях
	Проработка лекционного материала	1		
	Итого	5		
4 Организация защиты информации в Германии.	Подготовка к практическим занятиям, семинарам	4	ОК-5, ПК-9	Выступление (доклад) на занятии, Зачет, Конспект самоподготовки, Опрос на занятиях
	Проработка лекционного материала	1		
	Итого	5		
5 Организация защиты информации в Великобритании.	Подготовка к практическим занятиям, семинарам	4	ОК-5, ПК-9	Выступление (доклад) на занятии, Зачет, Конспект самоподготовки, Опрос на занятиях
	Проработка лекционного материала	1		
	Итого	5		
6 Организация защиты информации во Франции.	Подготовка к практическим занятиям, семинарам	4	ОК-5, ПК-9	Выступление (доклад) на занятии, Зачет, Конспект самоподготовки, Опрос на занятиях
	Проработка лекционного материала	1		
	Итого	5		
7 Организация защиты информации в Японии.	Подготовка к практическим занятиям, семинарам	4	ОК-5, ПК-9	Выступление (доклад) на занятии, Зачет, Конспект самоподготовки, Опрос на занятиях
	Проработка лекционного материала	1		

Согласована на портале № 19215

	Итого	5		
8 Организация защиты информации в КНР.	Подготовка к практическим занятиям, семинарам	4	ОК-5, ПК-9	Выступление (доклад) на занятии, Зачет, Конспект самоподготовки, Опрос на занятиях
	Проработка лекционного материала	1		
	Итого	5		
9 Стандарты информационной безопасности.	Подготовка к практическим занятиям, семинарам	5	ОК-5, ПК-9	Выступление (доклад) на занятии, Зачет, Конспект самоподготовки, Опрос на занятиях
	Проработка лекционного материала	1		
	Итого	6		
10 Международное сотрудничество в области защиты информации.	Подготовка к практическим занятиям, семинарам	2	ОК-5, ПК-9	Выступление (доклад) на занятии, Зачет, Конспект самоподготовки, Опрос на занятиях
	Проработка лекционного материала	1		
	Итого	3		
11 Информационное противоборство в системе международных отношений.	Подготовка к практическим занятиям, семинарам	2	ОК-5, ПК-9	Выступление (доклад) на занятии, Зачет, Конспект самоподготовки, Опрос на занятиях
	Проработка лекционного материала	1		
	Итого	3		
Итого за семестр		48		
Итого		48		

10. Курсовая работа (проект)

Не предусмотрено РУП

11. Рейтинговая система для оценки успеваемости студентов

11.1. Балльные оценки для элементов контроля

Таблица 11.1 – Балльные оценки для элементов контроля

Элементы учебной деятельности	Максимальный балл на 1-ую КТ с начала семестра	Максимальный балл за период между 1КТ и 2КТ	Максимальный балл за период между 2КТ и на конец семестра	Всего за семестр
7 семестр				
Выступление (доклад) на занятии	5	10	10	25
Зачет	10	10	20	40
Конспект самоподготовки	5	7	8	20
Опрос на занятиях	3	5	7	15
Итого максимум за пери-	23	32	45	100

Согласована на портале № 19215

од				
Нарастающим итогом	23	55	100	100

11.2. Пересчет баллов в оценки за контрольные точки

Пересчет баллов в оценки за контрольные точки представлен в таблице 11.2.

Таблица 11. 2 – Пересчет баллов в оценки за контрольные точки

Баллы на дату контрольной точки	Оценка
≥ 90% от максимальной суммы баллов на дату КТ	5
От 70% до 89% от максимальной суммы баллов на дату КТ	4
От 60% до 69% от максимальной суммы баллов на дату КТ	3
< 60% от максимальной суммы баллов на дату КТ	2

11.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 11.3.

Таблица 11. 3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка (ГОС)	Итоговая сумма баллов, учитывает успешно сданный экзамен	Оценка (ECTS)
5 (отлично) (зачтено)	90 - 100	A (отлично)
4 (хорошо) (зачтено)	85 - 89	B (очень хорошо)
	75 - 84	C (хорошо)
	70 - 74	D (удовлетворительно)
3 (удовлетворительно) (зачтено)	65 - 69	
	60 - 64	E (посредственно)
2 (неудовлетворительно) (не зачтено)	Ниже 60 баллов	F (неудовлетворительно)

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. Защита информации в инфокоммуникационных системах и сетях: Учебное пособие / Голиков А. М. - 2015. 284 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/5262, дата обращения: 01.05.2017.

12.2. Дополнительная литература

1. Защита интеллектуальной собственности в России: Учебное пособие / Сычев А. Н. - 2012. 241 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/2276, дата обращения: 01.05.2017.

12.3 Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Организационное обеспечение информационной безопасности: Методические указания для практических занятий / Белицкая Л. А. - 2011. 22 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/3030, дата обращения: 01.05.2017.
2. Защита информации: Методические указания к выполнению самостоятельных работ / Спицын В. Г. - 2012. 78 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/2261, дата обращения: 01.05.2017.

12.3.2 Учебно-методические пособия для лиц с ограниченными возможностями здоровья

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и

Согласована на портале № 19215

восприятия информации.

Для лиц с нарушениями зрения:

– в форме электронного документа;
– в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

– в форме электронного документа;
– в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

– в форме электронного документа;
– в печатной форме.

12.4. Базы данных, информационно-справочные, поисковые системы и требуемое программное обеспечение

1. 1. Базовые законодательные и нормативно-правовые документы РФ в области защиты информации. [Электронный ресурс]. - Режим доступа: http://www.consultant.ru, (дата обращения 25.04.2017);
2. 2. Научно-образовательный портал ТУСУРа, https://edu.tusur.ru

13. Материально-техническое обеспечение дисциплины

13.1. Общие требования к материально-техническому обеспечению дисциплины

13.1.1. Материально-техническое обеспечение для лекционных занятий

Лекционные, практические и лабораторные занятия проводятся в специализированных аудиториях кафедры РЗИ. Для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется учебная аудитория, с количеством посадочных мест не менее 22-24, оборудованная доской и стандартной учебной мебелью. Имеются наглядные пособия в виде презентаций по лекционным разделам дисциплины.

13.1.2. Материально-техническое обеспечение для практических занятий

Для проведения практических (семинарских) занятий используется учебные аудитории, расположенная по адресу 634034, Томская область, г. Томск, Вершинина улица, д. 47, 4 этаж, ауд. 407, 412, 416. Состав оборудования: Учебная мебель; Доска магнитно-маркерная -1шт.; Коммутатор D-Link Switch 24 port - 1шт.; Компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. -14 шт. Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows XP Professional with SP3/Microsoft Windows 7 Professional with SP1; Microsoft Windows Server 2008 R2; Visual Studio 2008 EE with SP1; Microsoft Office Visio 2010; Microsoft Office Access 2003; VirtualBox 6.2. Имеется помещения для хранения и профилактического обслуживания учебного оборудования.

13.1.3. Материально-техническое обеспечение для самостоятельной работы

Для самостоятельной работы используется учебная аудитория (компьютерный класс), расположенная по адресу 634034, г. Томск, ул. Вершинина, 47, 4 этаж, ауд. 407,412, 416. Состав оборудования: учебная мебель; компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 4 шт.; компьютеры подключены к сети ИНТЕРНЕТ и обеспечивают доступ в электронную информационно-образовательную среду университета.

13.2. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения.

При обучении студентов **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах для студентов с нарушениями слуха, мобильной системы обучения для студентов с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой обучаются студенты с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При обучении студентов **с нарушениями зрениями** предусмотрено использование в лекци-

Согласована на портале № 19215

онных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для удаленного просмотра.

При обучении студентов **с нарушениями опорно-двигательного аппарата** используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах для студентов с нарушениями опорно-двигательного аппарата, мобильной системы обучения для людей с инвалидностью.

14. Фонд оценочных средств

14.1. Основные требования к фонду оценочных средств и методические рекомендации

Фонд оценочных средств и типовые контрольные задания, используемые для оценки сформированности и освоения закрепленных за дисциплиной компетенций при проведении текущей, промежуточной аттестации по дисциплине приведен в приложении к рабочей программе.

14.2 Требования к фонду оценочных средств для лиц с ограниченными возможностями здоровья

Для студентов с инвалидностью предусмотрены дополнительные оценочные средства, перечень которых указан в таблице.

Таблица 14 – Дополнительные средства оценивания для студентов с инвалидностью

Категории студентов	Виды дополнительных оценочных средств	Формы контроля и оценки результатов обучения
С нарушениями слуха	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы	Преимущественно письменная проверка
С нарушениями зрения	Собеседование по вопросам к зачету, опрос по терминам	Преимущественно устная проверка (индивидуально)
С нарушениями опорно-двигательного аппарата	Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету	Преимущественно дистанционными методами
С ограничениями по общемедицинским показаниям	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы	Преимущественно проверка методами, исходя из состояния обучающегося на момент проверки

14.3 Методические рекомендации по оценочным средствам для лиц с ограниченными возможностями здоровья

Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной форме;
- в печатной форме с увеличенным шрифтом;
- в форме электронного документа;
- методом чтения ассистентом задания вслух;
- предоставление задания с использованием сурдоперевода.

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге;
- набор ответов на компьютере;
- набор ответов с использованием услуг ассистента;
- представление ответов устно.

Процедура оценивания результатов обучения инвалидов по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Согласована на портале № 19215

Для лиц с нарушениями зрения:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

Согласована на портале № 19215

Приложение 1

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. Е. Троян
«___» _____ 20__ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Системы защиты информации в ведущих зарубежных странах

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки (специальность): **10.03.01 Информационная безопасность**
Направленность (профиль): **Организация и технология защиты информации**
Форма обучения: **очная**
Факультет: **РТФ, Радиотехнический факультет**
Кафедра: **РЗИ, Кафедра радиоэлектроники и защиты информации**
Курс: **4**
Семестр: **7**

Учебный план набора 2013 года

Разработчик:
- доцент каф. РЗИ А. П. Кшнянкин

Зачет: 7 семестр

Томск 2017

Согласована на портале № 19215

1. Введение

Фонд оценочных средств (ФОС) является приложением к рабочей программе дисциплины (практики) и представляет собой совокупность контрольно-измерительных материалов (типовые задачи (задания), контрольные работы, тесты и др.) и методов их использования, предназначенных для измерения уровня достижения студентом установленных результатов обучения.

ФОС по дисциплине (практике) используется при проведении текущего контроля успеваемости и промежуточной аттестации студентов.

Перечень закрепленных за дисциплиной (практикой) компетенций приведен в таблице 1.

Таблица 1 – Перечень закрепленных за дисциплиной компетенций

Код	Формулировка компетенции	Этапы формирования компетенций
ПК-9	способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Должен знать • основные требования к безопасности информационных систем в США, странах Евросоюза, Японии и Китае. • историю создания систем защиты информации в США, странах Евросоюза, Японии и Китае. • порядок контроля и координации деятельности органов защиты информации в США, странах Евросоюза, Японии и Китае, особенности защиты государственной тайны в этих странах. • организацию информационно-психологического обеспечения современных военных конфликтов в США. • основные направления Национального плана по защите информационных систем в США. • характеристики основных положений Европейской директивы по защите данных. • особенности международного сотрудничества в области информационной безопасности в мире. • характеристики основных объектов и средств физической защиты, применяемых ведущими зарубежными странами в системе защиты территорий и помещений. основные международные стандарты информационной безопасности ; Должен уметь • классифицировать различные объекты и средства, определять требования к их защите на объектах информатизации ведущих зарубежных стран в том числе и от утечки по техническим каналам; • проводить анализ защищённости объектов и определять класс защиты информации по международным стандартам; • формулировать рекомендации по увеличению уровня защищённости российских объектов информатизации на основе опыта защиты информации в ведущих за рубежных странах. ; Должен владеть • навыками использования систем защиты информации в веду-
ОК-5	способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	

Согласована на портале № 19215

		щих зарубежных странах при обеспечении информационной безопасности предприятий. ;

Общие характеристики показателей и критериев оценивания компетенций на всех этапах приведены в таблице 2.

Таблица 2 – Общие характеристики показателей и критериев оценивания компетенций по этапам

Показатели и критерии	Знать	Уметь	Владеть
Отлично (высокий уровень)	Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости	Обладает диапазоном практических умений, требуемых для развития творческих решений, абстрагирования проблем	Контролирует работу, проводит оценку, совершенствует действия работы
Хорошо (базовый уровень)	Знает факты, принципы, процессы, общие понятия в пределах изучаемой области	Обладает диапазоном практических умений, требуемых для решения определенных проблем в области исследования	Берет ответственность за завершение задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем
Удовлетворительно (пороговый уровень)	Обладает базовыми общими знаниями	Обладает основными умениями, требуемыми для выполнения простых задач	Работает при прямом наблюдении

2 Реализация компетенций

2.1 Компетенция ПК-9

ПК-9: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 3.

Таблица 3 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	• основные требования к безопасности информационных систем в США, странах Евро-союза, Японии и Китае. • историю создания систем защиты информации в США, странах Евросоюза, Японии и Китае. • порядок контроля и координации деятельности органов защиты информации в США, странах Евросоюза, Японии и Китае, особенности защиты государственной тайны в этих странах. • организацию информа-	• классифицировать различные объекты и средства, определять требования к их защите на объектах информатизации ведущих зарубежных стран в том числе и от утечки по техническим каналам; • проводить анализ защищённости объектов и определять класс защиты информации по международным стандартам; • формулировать рекомендации по увеличению уровня защищённости российских объектов ин-	• навыками использования систем защиты информации в ведущих зарубежных странах при обеспечении информационной безопасности предприятий

Согласована на портале № 19215

	ционно-психологического обеспечения современных военных конфликтов в США. • основные направления Национального плана по защите информационных систем в США. • характеристики основных положений Европейской директивы по защите данных. • особенности международного сотрудничества в области информационной безопасности в мире. • характеристики основных объектов и средств физической защиты, применяемых ведущими зарубежными странами в системе защиты территорий и помещений. основные международные стандарты информационной безопасности	форматизации на основе опыта защиты информации в ведущих зарубежных странах.	
Виды занятий	• Интерактивные практические занятия; • Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Самостоятельная работа;
Используемые средства оценивания	• Конспект самоподготовки; • Опрос на занятиях; • Выступление (доклад) на занятии; • Зачет;	• Конспект самоподготовки; • Опрос на занятиях; • Выступление (доклад) на занятии; • Зачет;	• Выступление (доклад) на занятии; • Зачет;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 4.

Таблица 4 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости.;	• Обладает диапазоном практических умений, требуемых для развития творческих решений, абстрагирования проблем.;	• Контролирует работу, проводит оценку, совершенствует действия работы.;

Согласована на портале № 19215

Хорошо (базовый уровень)	• Знает факты, принципы, процессы, общие понятия в пределах изучаемой области.;	• Обладает диапазоном практических умений, требуемых для решения определенных проблем в области исследования. ;	• Берет ответственность за завершение задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем. ;
Удовлетворительно (пороговый уровень)	• Обладает базовыми общими знаниями.;	• Обладает основными умениями, требуемыми для выполнения простых задач.;	• Работает при прямом наблюдении.;

2.2 Компетенция ОК-5

ОК-5: способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 5.

Таблица 5 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	• основные требования к безопасности информационных систем в США, странах Евро-союза, Японии и Китае. • историю создания систем защиты информации в США, странах Евросоюза, Японии и Китае. • порядок контроля и координации деятельности органов защиты информации в США, странах Евросоюза, Японии и Китае, особенности защиты государственной тайны в этих странах. • организацию информационно-психологического обеспечения современных военных конфликтов в США. • основные направления Национального плана по защите информационных систем в США. • характеристики основных положений Европейской директивы по защите данных. • особенности международного сотрудниче-	• классифицировать различные объекты и средства, определять требования к их защите на объектах информатизации ведущих зарубежных стран в том числе и от утечки по техническим каналам; • проводить анализ защищённости объектов и определять класс защиты информации по международным стандартам; • формулировать рекомендации по увеличению уровня защищённости российских объектов информатизации на основе опыта защиты информации в ведущих зарубежных странах.	• навыками использования систем защиты информации в ведущих зарубежных странах при обеспечении информационной безопасности предприятий.

Согласована на портале № 19215

	ства в области информационной безопасности в мире. • характеристики основных объектов и средств физической защиты, применяемых ведущими зарубежными странами в системе защиты территорий и помещений. основные международные стандарты информационной безопасности.		
Виды занятий	• Интерактивные практические занятия; • Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Самостоятельная работа;
Используемые средства оценивания	• Конспект самоподготовки; • Опрос на занятиях; • Выступление (доклад) на занятии; • Зачет;	• Конспект самоподготовки; • Опрос на занятиях; • Выступление (доклад) на занятии; • Зачет;	• Выступление (доклад) на занятии; • Зачет;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 6.

Таблица 6 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости.;	• Обладает диапазоном практических умений, требуемых для развития творческих решений, абстрагирования проблем.;	• Контролирует работу, проводит оценку, совершенствует действия работы.;
Хорошо (базовый уровень)	• Знает факты, принципы, процессы, общие понятия в пределах изучаемой области.;	• Обладает диапазоном практических умений, требуемых для решения определенных проблем в области исследования. ;	• Берет ответственность за завершение задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем. ;
Удовлетворительно (пороговый уровень)	• Обладает базовыми общими знаниями.;	• Обладает основными умениями, требуемыми для выполнения простых задач.;	• Работает при прямом наблюдении.;

Согласована на портале № 19215

3 Типовые контрольные задания

Для реализации вышеперечисленных задач обучения используются 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, в следующем составе.

3.1 Вопросы на самоподготовку

– • Особенности опыта организации защиты информации на Древнем Востоке. История основных направлений, принципов и методов защиты информации в средневековой Европе. Создание первых европейских государственных секретных служб (на примере Англии, Франции, Германии). Опыт криптографической защиты информации в странах Западной Европы. Методы защиты коммерческих сведений. Формирование особенностей политики защиты государственных секретов и коммерческой тайны в странах Западной Европы, США и Японии в XVIII – XX в.в. Разведка и контрразведка как элементы политики обеспечения безопасности государств. Промышленный шпионаж: его значение для формирования систем защиты информации. Особенности государственной политики по отношению к промышленному шпионажу в национальных и межгосударственных рамках. Формирование авторского и патентного права. Особенности формирования современных систем защиты информации в ведущих зарубежных странах в XXI в.

– • Государственная политика в области защиты информации. Организация защиты информации по национальной безопасности (государственных секретов). Состав и основные функции органов, осуществляющих защиту информации по национальной безопасности. Особенности организации защиты информации в промышленности. Защита секретной информации, используемой в международных программах. Доступ к правительственной информации. Порядок предоставления доступа к информации лицам, не являющимся гражданами США. Организация защиты коммерческой тайны. Классификация информации, составляющей коммерческую тайну. Доступ к информации, принадлежащей частным лицам. Организация контроля надежности функционирования системы защиты коммерческой тайны фирмы. Требования к персоналу. Особенности подбора, проверки, подготовки, текущей работы с персоналом, допущенным к информации, составляющей коммерческую тайну фирмы.

– • Государственная политика в области защиты информации. Организация системы специальных служб в области защиты информации. Парламентско-правительственный контроль за деятельностью специальных служб. Состав, структура и основные направления деятельности служб безопасности. Общественные организации по борьбе с экономическим шпионажем и преступностью. Взаимодействие системы специальных служб и правоохранительных органов с частными промышленными и коммерческими службами безопасности. Особенности подбора, проверки, профессиональной подготовки, текущей работы с персоналом, допущенным к защищаемой информации. Особенности защиты информации в банковской сфере. Правовые основы защиты информации. Государственная тайна и доступ к правительственной, парламентской и судебной информации. Правовая защита служебной, налоговой тайны, тайны судебного разбирательства, тайны почтовых и телесообщений, коммерческой и производственной тайны. Организация доступа к информации, принадлежащей частным лицам.

– • Государственная политика в области защиты информации. Организация системы специальных служб и их основные функции в области защиты информации. Функции специальных подразделений министерства торговли и промышленности по предупреждению коммерческих преступлений. Особенности подбора, проверки, профессиональной подготовки, текущей работы с персоналом, допущенным к защищаемой информации. Содержание программы обеспечения безопасности предприятия. Особенности защиты информации и предупреждение компьютерных преступлений в банковской сфере. Классификация защищаемой информации. Правовые основы защиты информации. Государственная тайна и организация доступа к правительственной информации. Правовая защита тайны корреспонденции. Коммерческая тайна и доступ к информации, принадлежащей частным лицам.

– • Государственная политика в области защиты информации. Организация системы специальных служб и их основные функции в области защиты информации. Службы безопасности в промышленно-торговых фирмах и финансовых учреждениях (банках, страховых компаниях, инвестиционных фирмах). Службы безопасности в фирмах, выполняющих государственные заказы в

Согласована на портале № 19215

сфере оборонной промышленности, космических и ядерных исследований, новых видов вооружений, средств связи и транспорта. Особенности подбора, проверки, профессиональной подготовки, текущей работы с персоналом, допущенным к защищаемой информации. Особенности защиты информации в банковской сфере. Правовые основы защиты информации. Государственная тайна и организация доступа к правительственной информации, парламентским заседаниям, публикация парламентских документов. Правовая защита служебной, профессиональной тайны, тайны корреспонденции. Коммерческая тайна и организация доступа к информации, принадлежащей частным предприятиям.

– • Государственная политика в области защиты информации. Организация системы специальных служб и их функции в области защиты информации. Общественные организации, оказывающие помощь органам полиции в сфере защиты экономической информации (территориальные советы по предупреждению преступности, общества содействия полиции, пункты связи по предупреждению преступности). Службы безопасности отдельных организаций. Подразделения внутреннего самоконтроля отдельных организаций и их функции в сфере защиты информации. Особенности подбора, проверки, профессиональной подготовки, текущей работы с персоналом, допущенным к защищаемой информации. Принцип корпоративной защиты и обеспечения безопасности объекта. Защита информации в процессе взаимодействия фирм с иностранными партнерами. Правовые основы защиты информации.

– • Представление об информационном противоборстве в Китае. Государственная политика в области защиты информации. Организация системы специальных служб и их функции в области защиты информации. Организационная структура спецслужб Китая. Законодательство в сфере информационной безопасности в Китае. «Великая стена» информационной безопасности Китае.

– • Предпосылки создания стандартов информационной безопасности. Стандарт «Критерии оценки надежности компьютерных систем» (Оранжевая книга). Гармонизированные критерии европейских стран. Германский стандарт BSI. Британский стандарт BS 7799. Международный стандарт ISO 17799. Международный стандарт ISO 15408 «Общие критерий». Стандарт COBIT.

– • Научно-техническое сотрудничество с зарубежными партнерами. Организация защиты информации в процессе проведения международных конференций, симпозиумов, обмена специалистами и др. Регламентация процедур обеспечения защиты информации в ходе посещения представителями зарубежных фирм охраняемых объектов. Порядок предоставления защищаемой информации другим странам. Международный опыт защиты информации в процессе банковской деятельности. Международный опыт стандартизации в области защиты информации. Международная защита интеллектуальной собственности. Международные договоры и иные международно-правовые документы (Всеобщая декларация прав человека, Международный пакт о гражданских и политических правах, Договор об образовании Европейского экономического сообщества и др.) о защите информации, предупреждении недобросовестной конкуренции в процессе международного предпринимательства, предупреждении компьютерных преступлений.

– • Современная картина международных отношений в мире. Основы информационно-психологического воздействия. Типы информационного оружия.

3.2 Зачёт

– История развитие систем защиты информации в ведущих зарубежных странах.
– Организация защиты информации в США.
– Организация защиты информации в Германии.
– Организация защиты информации в Великобритании.
– Организация защиты информации во Франции.
– Организация защиты информации в Японии.
– Организация защиты информации в КНР.
– Стандарты информационной безопасности.
– Международное сотрудничество в области защиты информации.
– Информационное противоборство в системе международных отношений.

3.3 Темы опросов на занятиях

– Предмет и задачи курса. Взаимосвязь курса с другими дисциплинами. Разделы и темы,

Согласована на портале № 19215

их распределение по видам аудиторных занятий. Формы проведения семинарских занятий. Состав самостоятельной работы студентов по изучению дисциплины. Анализ нормативных источников, научной и учебной литературы.

– Особенности опыта организации защиты информации на Древнем Востоке. История основных направлений, принципов и методов защиты информации в средневековой Европе. Создание первых европейских государственных секретных служб (на примере Англии, Франции, Германии). Опыт криптографической защиты информации в странах Западной Европы. Методы защиты коммерческих сведений. Формирование особенностей политики защиты государственных секретов и коммерческой тайны в странах Западной Европы, США и Японии в XVIII – XX в.в. Разведка и контрразведка как элементы политики обеспечения безопасности государств. Промышленный шпионаж: его значение для формирования систем защиты информации. Особенности государственной политики по отношению к промышленному шпионажу в национальных и межгосударственных рамках. Формирование авторского и патентного права. Особенности формирования современных систем защиты информации в ведущих зарубежных странах в XXI в.

– Государственная политика в области защиты информации. Организация защиты информации по национальной безопасности (государственных секретов). Состав и основные функции органов, осуществляющих защиту информации по национальной безопасности. Особенности организации защиты информации в промышленности. Защита секретной информации, используемой в международных программах. Доступ к правительственной информации. Порядок предоставления доступа к информации лицам, не являющимся гражданами США. Организация защиты коммерческой тайны. Классификация информации, составляющей коммерческую тайну. Доступ к информации, принадлежащей частным лицам. Организация контроля надежности функционирования системы защиты коммерческой тайны фирмы. Требования к персоналу. Особенности подбора, проверки, подготовки, текущей работы с персоналом, допущенным к информации, составляющей коммерческую тайну фирмы.

– Государственная политика в области защиты информации. Организация системы специальных служб в области защиты информации. Парламентско-правительственный контроль за деятельностью специальных служб. Состав, структура и основные направления деятельности служб безопасности. Общественные организации по борьбе с экономическим шпионажем и преступностью. Взаимодействие системы специальных служб и правоохранительных органов с частными промышленными и коммерческими службами безопасности. Особенности подбора, проверки, профессиональной подготовки, текущей работы с персоналом, допущенным к защищаемой информации. Особенности защиты информации в банковской сфере. Правовые основы защиты информации. Государственная тайна и доступ к правительственной, парламентской и судебной информации. Правовая защита служебной, налоговой тайны, тайны судебного разбирательства, тайны почтовых и телесообщений, коммерческой и производственной тайны. Организация доступа к информации, принадлежащей частным лицам.

– Государственная политика в области защиты информации. Организация системы специальных служб и их основные функции в области защиты информации. Функции специальных подразделений министерства торговли и промышленности по предупреждению коммерческих преступлений. Особенности подбора, проверки, профессиональной подготовки, текущей работы с персоналом, допущенным к защищаемой информации. Содержание программы обеспечения безопасности предприятия. Особенности защиты информации и предупреждение компьютерных преступлений в банковской сфере. Классификация защищаемой информации. Правовые основы защиты информации. Государственная тайна и организация доступа к правительственной информации. Правовая защита тайны корреспонденции. Коммерческая тайна и доступ к информации, принадлежащей частным лицам.

– Государственная политика в области защиты информации. Организация системы специальных служб и их основные функции в области защиты информации. Службы безопасности в промышленно-торговых фирмах и финансовых учреждениях (банках, страховых компаниях, инвестиционных фирмах). Службы безопасности в фирмах, выполняющих государственные заказы в сфере оборонной промышленности, космических и ядерных исследований, новых видов вооружений, средств связи и транспорта. Особенности подбора, проверки, профессиональной подготовки, текущей работы с персоналом, допущенным к защищаемой информации. Особенности защиты ин-

Согласована на портале № 19215

формации в банковской сфере. Правовые основы защиты информации. Государственная тайна и организация доступа к правительственной информации, парламентским заседаниям, публикация парламентских документов. Правовая защита служебной, профессиональной тайны, тайны корреспонденции. Коммерческая тайна и организация доступа к информации, принадлежащей частным предприятиям.

– Государственная политика в области защиты информации. Организация системы специальных служб и их функции в области защиты информации. Общественные организации, оказывающие помощь органам полиции в сфере защиты экономической информации (территориальные советы по предупреждению преступности, общества содействия полиции, пункты связи по предупреждению преступности). Службы безопасности отдельных организаций. Подразделения внутреннего самоконтроля отдельных организаций и их функции в сфере защиты информации. Особенности подбора, проверки, профессиональной подготовки, текущей работы с персоналом, допущенным к защищаемой информации. Принцип корпоративной защиты и обеспечения безопасности объекта. Защита информации в процессе взаимодействия фирм с иностранными партнерами. Правовые основы защиты информации.

– Представление об информационном противоборстве в Китае. Государственная политика в области защиты информации. Организация системы специальных служб и их функции в области защиты информации. Организационная структура спецслужб Китая. Законодательство в сфере информационной безопасности в Китае. «Великая стена» информационной безопасности Китае.

– Предпосылки создания стандартов информационной безопасности. Стандарт «Критерии оценки надежности компьютерных систем» (Оранжевая книга). Гармонизированные критерии европейских стран. Германский стандарт BSI. Британский стандарт BS 7799. Международный стандарт ISO 17799. Международный стандарт ISO 15408 «Общие критерий». Стандарт COBIT.

– Научно-техническое сотрудничество с зарубежными партнерами. Организация защиты информации в процессе проведения международных конференций, симпозиумов, обмена специалистами и др. Регламентация процедур обеспечения защиты информации в ходе посещения представителями зарубежных фирм охраняемых объектов. Порядок предоставления защищаемой информации другим странам. Международный опыт защиты информации в процессе банковской деятельности. Международный опыт стандартизации в области защиты информации. Международная защита интеллектуальной собственности. Международные договоры и иные международно-правовые документы (Всеобщая декларация прав человека, Международный пакт о гражданских и политических правах, Договор об образовании Европейского экономического сообщества и др.) о защите информации, предупреждении недобросовестной конкуренции в процессе международного предпринимательства, предупреждении компьютерных преступлений.

– Современная картина международных отношений в мире. Основы информационно-психологического воздействия. Типы информационного оружия.

3.4 Темы докладов

– История развитие систем защиты информации в ведущих зарубежных странах.
– Организация защиты информации в США.
– Организация защиты информации в Германии.
– Организация защиты информации в Великобритании.
– Организация защиты информации во Франции.
– Организация защиты информации в Японии.
– Организация защиты информации в КНР.
– Стандарты информационной безопасности.
– Международное сотрудничество в области защиты информации.
– Информационное противоборство в системе международных отношений.

4 Методические материалы

Для обеспечения процесса обучения и решения задач обучения используются следующие материалы:

– методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы фор-мирования компетенций, согласно п.

Согласована на портале № 19215

12 рабочей программы.

4.1. Основная литература

1. Защита информации в инфокоммуникационных системах и сетях: Учебное пособие / Голиков А. М. - 2015. 284 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/5262, свободный.

4.2. Дополнительная литература

1. Защита интеллектуальной собственности в России: Учебное пособие / Сычев А. Н. - 2012. 241 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/2276, свободный.

4.3. Обязательные учебно-методические пособия

1. Организационное обеспечение информационной безопасности: Методические указания для практических занятий / Белицкая Л. А. - 2011. 22 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/3030, свободный.
2. Защита информации: Методические указания к выполнению самостоятельных работ / Спицын В. Г. - 2012. 78 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/2261, свободный.

4.4. Базы данных, информационно справочные и поисковые системы

1. 1. Базовые законодательные и нормативно-правовые документы РФ в области защиты информации. [Электронный ресурс]. - Режим доступа: http://www.consultant.ru, (дата обращения 25.04.2017);
2. 2. Научно-образовательный портал ТУСУРа, https://edu.tusur.ru

Согласована на портале № 19215