МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Организационное и правовое обеспечение информационной безопасности

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **10.05.02 Информационная безопасность телекоммуникационных систем**
Направленность (профиль) / специализация: **Защита информации в системах связи и управления**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **БИС, Кафедра безопасности информационных систем**
Курс: **3**
Семестр: **5**
Учебный план набора 2020 года

Распределение рабочего времени

№	Виды учебной деятельности	5 семестр	Всего	Единицы
1	Лекции	36	36	часов
2	Практические занятия	28	28	часов
3	Всего аудиторных занятий	64	64	часов
4	Самостоятельная работа	44	44	часов
5	Всего (без экзамена)	108	108	часов
6	Подготовка и сдача экзамена	36	36	часов
7	Общая трудоемкость	144	144	часов
		4.0	4.0	З.Е.

Экзамен: 5 семестр

Томск

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Цель – дать основы правового обеспечения информационной безопасности, а также формирование знаний по организационному обеспечению информационной безопасности и навыков по их определению для конкретных условий.

1.2. Задачи дисциплины

- Задачи дисциплины - дать основы:
- - законодательства РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации;
- -понятий и видов защищаемой информации по законодательству РФ;
- - правовых режимов конфиденциальной информации;
- - правового режим защиты государственной тайны, системы защиты государственной тайны;
- - лицензирования и сертификации в области защиты информации, в том числе государственной тайны;
- -правовых основ защиты информации с использованием технических средств (защита от технических разведок, применение и разработка шифровальных средств, электронная цифровая подпись и т.д.);
- -защиты интеллектуальной собственности;
- -правовой регламентации охранной деятельности;
- -правового регулирования взаимоотношений администрации и персонала в области защиты информации;
- - международного законодательства в области защиты информации;
- - знаний о преступлениях в сфере компьютерной информации, экспертизах преступлений в области компьютерной информации, криминалистических аспектах проведения расследований.
- -угроз информационной безопасности объекта;
- -организации службы безопасности объекта;
- - подбора и работы с кадрами в сфере информационной безопасности;
- - организации и обеспечения режима конфиденциальности;
- -охраны объектов.
-

2. Место дисциплины в структуре ОПОП

Дисциплина «Организационное и правовое обеспечение информационной безопасности» (Б1.Б.09.01) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Основы информационной безопасности.

Последующими дисциплинами являются: Техническая защита информации.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ОПК-7 способностью применять нормативные правовые акты в своей профессиональной деятельности;
- ПК-10 способностью оценивать выполнение требований нормативных правовых актов и нормативных методических документов в области информационной безопасности при проверке защищенных телекоммуникационных систем, выполнять подготовку соответствующих заключений;
- ПК-13 способностью организовывать выполнение требований режима защиты информации ограниченного доступа, разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности телекоммуникационных систем;

В результате изучения дисциплины обучающийся должен:

– **знать** − основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; − правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях; − организацию работы и нормативные правовые акты, и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; − информационные технологии, используемые в автоматизированных системах.

– **уметь** − применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; − разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации.

– **владеть** − профессиональной терминологией в области информационной безопасности; − навыками работы с нормативными правовыми актами; − навыками организации и обеспечения режима секретности; − методами организации и управления деятельностью служб защиты информации на предприятии; - методами формирования требований по защите информации.

4. Название разделов (тем) дисциплины

Названия разделов дисциплины
5 семестр
1 Законодательство РФ в области информационной безопасности.
2 Правовые основы защиты конфиденциальной информации.
3 Правовые основы защиты государственной тайны.
4 Лицензирование и сертификация.
5 Нормы ответственности за правонарушения в сфере компьютерных технологий.
6 Анализ объекта защиты с позиции организационного обеспечения информационной безопасности.
7 Средства и методы физической защиты объектов.
8 Организация службы безопасности и работа с кадрами.
9 Организация и обеспечения режима секретности.
10 Организация пропускного и внутри объектового режима.