

Документ подписан электронной подписью
Информация о владельце:
ФИО: Сенченко Павел Васильевич
Должность: Проректор по учебной работе
Дата подписания: 29.09.2023 07:29:30
Уникальный программный ключ:
27e516f4c088deb62ba68945f4406e13fd454355

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: **38.05.01 Экономическая безопасность**

Направленность (профиль) / специализация: **Экономико-правовое обеспечение экономической безопасности**

Форма обучения: **заочная**

Факультет: **ЗиВФ, Заочный и вечерний факультет**

Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**

Курс: **3, 4**

Семестр: **6, 7**

Учебный план набора 2013 года

Распределение рабочего времени

№	Виды учебной деятельности	6 семестр	7 семестр	Всего	Единицы
1	Лекции	4	4	8	часов
2	Практические занятия	2	4	6	часов
3	Всего аудиторных занятий	6	8	14	часов
4	Из них в интерактивной форме	2	4	6	часов
5	Самостоятельная работа	66	55	121	часов
6	Всего (без экзамена)	72	63	135	часов
7	Подготовка и сдача экзамена	0	9	9	часов
8	Общая трудоемкость	72	72	144	часов
				4.0	З.Е.

Контрольные работы: 7 семестр - 1

Экзамен: 7 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.В.ОД.4) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Организационное и правовое обеспечение информационной безопасности, Основы информационной безопасности, Правоведение.

Последующими дисциплинами являются: Организационное и правовое обеспечение информационной безопасности, Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ПК-20 способностью соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности;
 - ПСК-1 способностью составлять соответствующие юридические документы и обосновывать решения, связанные с реализацией правовых норм в пределах должностных обязанностей;
- В результате изучения дисциплины обучающийся должен:
- **знать** – основы организационного и правового обеспечения информационной безопас-

ности, 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
6 семестр
1 Законодательство РФ в области информационной безопасности.
2 Правовые основы защиты конфиденциальной информации.
3 Правовые основы защиты государственной тайны.
4 Нормы ответственности за правонарушения в сфере компьютерных технологий.
7 семестр
5 Средства и методы физической защиты объектов.
6 Организация службы безопасности и работа с кадрами.
7 Организация и обеспечения режима секретности.
8 Организация пропускного и внутри объектового режима.