

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Сенченко Павел Васильевич
Должность: Проректор по учебной работе
Дата подписания: 26.09.2023 11:06:09
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

Нормативное обеспечение защиты информации

Уровень образования: **высшее образование - специалитет**

Направление подготовки / специальность: **10.05.03 Информационная безопасность автоматизированных систем**

Направленность (профиль) / специализация: **Информационная безопасность автоматизированных банковских систем**

Форма обучения: **очная**

Факультет: **ФБ, Факультет безопасности**

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

Курс: **4**

Семестр: **8**

Учебный план набора 2020 года

Распределение рабочего времени

№	Виды учебной деятельности	8 семестр	Всего	Единицы
1	Лекции	18	18	часов
2	Практические занятия	36	36	часов
3	Всего аудиторных занятий	54	54	часов
4	Самостоятельная работа	90	90	часов
5	Всего (без экзамена)	144	144	часов
6	Подготовка и сдача экзамена	36	36	часов
7	Общая трудоемкость	180	180	часов
		5.0	5.0	З.Е.

Экзамен: 8 семестр

Томск

1. Цели и задачи дисциплины

1.1. Цели дисциплины

формирование знаний по организационному обеспечению информационной безопасности и навыков по их определению для конкретных условий.

1.2. Задачи дисциплины

- дать актуальные знания по законодательству РФ в области информационной безопасности, защите персональных данных и критической информационной инфраструктуры;
- дать актуальные знания по международному законодательству в области защиты информации.
-
-

2. Место дисциплины в структуре ОПОП

Дисциплина «Нормативное обеспечение защиты информации» (Б1.В.02.03) относится к блоку 1 (вариативная часть).

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

Последующими дисциплинами являются: Преддипломная практика.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы;
- ПК-9 способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности;
- ПК-15 способностью участвовать в проведении экспериментально-исследовательских работ по сертификации средств защиты информации автоматизированных систем;
- ПК-16 способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации;
- ПК-21 способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных 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.
- **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

8 семестр

1 Нормативное обеспечение безопасности персональных данных
--

2 Нормативное обеспечение безопасности критической информационной инфраструктуры
--

3 Нормативное обеспечение по технической защите информации
--