

Документ подписан электронной подписью
Информация о владельце:
ФИО: Сенченко Павел Васильевич
Должность: Проректор по учебной работе
Дата подписания: 29.09.2023 07:29:28
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

Управление информационной безопасностью

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: **6**

Семестр: **11, 12**

Учебный план набора 2013 года

Распределение рабочего времени

№	Виды учебной деятельности	11 семестр	12 семестр	Всего	Единицы
1	Лекции	4	4	8	часов
2	Практические занятия	4	4	8	часов
3	Лабораторные работы	8	8	16	часов
4	Всего аудиторных занятий	16	16	32	часов
5	Из них в интерактивной форме	0	6	6	часов
6	Самостоятельная работа	56	47	103	часов
7	Всего (без экзамена)	72	63	135	часов
8	Подготовка и сдача экзамена	0	9	9	часов
9	Общая трудоемкость	72	72	144	часов
				4.0	З.Е.

Контрольные работы: 12 семестр - 1

Экзамен: 12 семестр

Томск

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Целью дисциплины является овладение основными принципами управления уровнем информационной безопасности защищаемых ресурсов организации.

1.2. Задачи дисциплины

- Получение студентами знаний о структуре и принципах построения политики информационной безопасности организации.
- Получение студентами умений и навыков по построению моделей угроз и нарушителей и по оценке рисков информационной безопасности в организации.
- Получение студентами знаний об основных методах контроля обеспечения информационной безопасности в организации.

2. Место дисциплины в структуре ОПОП

Дисциплина «Управление информационной безопасностью» (Б1.В.ОД.10) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Безопасность жизнедеятельности, Безопасность операционных систем, Документоведение, Организационное и правовое обеспечение информационной безопасности, Прикладная криптография, Управление информационной безопасностью.

Последующими дисциплинами являются: Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты, Преддипломная практика, Управление информационной безопасностью.

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;

В результате изучения дисциплины обучающийся должен:

- **знать** основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические); основные методы управления информационной безопасностью; принципы формирования политики информационной безопасности в автоматизированных системах
- **уметь** оценивать информационные риски в автоматизированных системах; определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем; составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем; разрабатывать частные политики информационной безопасности автоматизированных систем; контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем; разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем.
- **владеть** профессиональной терминологией в области информационной безопасности; навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем; методами управления информационной безопасностью автоматизированных систем; методами оценки информационных рисков; навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем.

4. Название разделов (тем) дисциплины

Названия разделов дисциплины
11 семестр
1 Анализ объекта защиты

2 Оценка рисков информационной безопасности
12 семестр
3 Управление инцидентами информационной безопасности
4 Система управления информационной безопасностью