

Документ подписан электронной подписью
Информация о владельце:
ФИО: Сенченко Павел Васильевич
Должность: Проректор по учебной работе
Дата подписания: 25.10.2023 08:17:17
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

Основы управления информационной безопасностью

Уровень образования: **высшее образование - бакалавриат**

Направление подготовки / специальность: **10.03.01 Информационная безопасность**

Направленность (профиль) / специализация: **Безопасность автоматизированных систем**

Форма обучения: **очная**

Факультет: **ФБ, Факультет безопасности**

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

Курс: **4**

Семестр: **7**

Учебный план набора 2020 года

Распределение рабочего времени

№	Виды учебной деятельности	7 семестр	Всего	Единицы
1	Лекции	28	28	часов
2	Практические занятия	18	18	часов
3	Лабораторные работы	12	12	часов
4	Всего аудиторных занятий	58	58	часов
5	Самостоятельная работа	86	86	часов
6	Всего (без экзамена)	144	144	часов
7	Подготовка и сдача экзамена	36	36	часов
8	Общая трудоемкость	180	180	часов
		5.0	5.0	З.Е.

Экзамен: 7 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 «Основы управления информационной безопасностью» (Б1.Б1.04.03) относится к блоку 1 (вариативная часть).

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

Последующими дисциплинами являются: Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты, Нормативное обеспечение защиты информации.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ОПК-7 способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты ;
- ПК-4 способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты ;
- ПК-7 способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений ;
- ПК-13 способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации ;
- ПК-14 способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности;

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 автоматизи-

рованных 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
7 семестр
1 Анализ объекта защиты
2 Внутренние угрозы ИБ
3 Подбор и увольнение сотрудников
4 Текущая работа с персоналом
5 Разграничение доступа и контроль работы сотрудников
6 Управление инцидентами ИБ
7 Системы менеджмента ИБ
8 Свод правил по управлению ИБ
9 Обеспечение защиты информации в экстренных ситуациях