

Документ подписан электронной подписью  
Информация о владельце:  
ФИО: Сенченко Павел Васильевич  
Должность: Проректор по учебной работе  
Дата подписания: 26.09.2023 12:44:25  
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**

**Принципы построения, проектирования и эксплуатации информационно-аналитических систем**

Уровень образования: **высшее образование - специалитет**

Направление подготовки / специальность: **10.05.04 Информационно-аналитические системы безопасности**

Направленность (профиль) / специализация: **Информационная безопасность финансовых и экономических структур**

Форма обучения: **очная**

Факультет: **ФБ, Факультет безопасности**

Кафедра: **БИС, Кафедра безопасности информационных систем**

Курс: **4, 5**

Семестр: **8, 9**

Учебный план набора 2020 года

**Распределение рабочего времени**

№	Виды учебной деятельности	8 семестр	9 семестр	Всего	Единицы
1	Лекции	20	30	50	часов
2	Практические занятия	30	30	60	часов
3	Всего аудиторных занятий	50	60	110	часов
4	Самостоятельная работа	58	48	106	часов
5	Всего (без экзамена)	108	108	216	часов
6	Подготовка и сдача экзамена	0	36	36	часов
7	Общая трудоемкость	108	144	252	часов
		3.0	4.0	7.0	З.Е.

Зачёт: 8 семестр

Экзамен: 9 семестр

Томск

## 1. Цели и задачи дисциплины

### 1.1. Цели дисциплины

Целью преподавания дисциплины является: освоение основных методов, используемых при работе с защищенными автоматизированными системами на этапах их разработки, реализации и эксплуатации.

### 1.2. Задачи дисциплины

- Задачами изучения дисциплины являются: дать студентам знания о способах проектирования и документального оформления процесса разработки защищенных автоматизированных систем на основе специализированных международных стандартов, развить в них умения и навыки применения специализированных международных стандартов при разработке средств защиты
- информации, умения и навыки в области разработки защищенных автоматизированных систем в соответствии с требованиями профиля защиты, а также дать знания о методах организации и регламентации процесса эксплуатации защищенных автоматизированных систем.

## 2. Место дисциплины в структуре ОПОП

Дисциплина «Принципы построения, проектирования и эксплуатации информационно-аналитических систем» (Б1.Б.05.05) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Принципы построения, проектирования и эксплуатации информационно-аналитических систем.

Последующими дисциплинами являются: Принципы построения, проектирования и эксплуатации информационно-аналитических систем.

## 3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ОПК-2 способностью корректно применять аппарат математического анализа, геометрии, алгебры, дискретной математики, теории вероятностей, математической статистики, численных методов, методов оптимизации для формализации и решения задач в сфере профессиональной деятельности;
- ПК-7 способностью проводить предпроектное обследование профессиональной деятельности и информационных потребностей автоматизируемых подразделений;
- ПК-10 способностью осуществлять выбор технологии, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности создаваемых специальных ИАС;
- ПК-11 способностью разрабатывать проектные документы на создаваемые специальные ИАС, в том числе средства обеспечения их информационной безопасности;
- ПК-12 способностью разрабатывать программное и иные виды обеспечения специальных ИАС;
- ПК-13 способностью оценивать эффективность специальных ИАС, в том числе средств обеспечения их информационной безопасности;
- ПК-15 способностью эксплуатировать специальные ИАС и средства обеспечения их информационной безопасности на всех этапах жизненного цикла, а также восстанавливать их работоспособность при внештатных ситуациях;
- ПК-16 способностью разрабатывать проекты нормативных, методических, организационно-распорядительных документов, регламентирующих функционирование специальных ИАС и средств обеспечения их информационной безопасности;

В результате изучения дисциплины обучающийся должен:

- **знать** – основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; – автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; – методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем;

ных систем и подсистем безопасности автоматизированных систем; – содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем; – методы, способы и средства обеспечения отказоустойчивости автоматизированных систем; – основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические); – основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах; – основные информационные технологии, используемые в автоматизированных системах

– **уметь** - разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем; - администрировать подсистемы информационной безопасности автоматизированных систем; - восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях; - исследовать эффективность создаваемых средств автоматизации, проводить техникоэкономическое обоснование проектных решений; - разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов; - определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; - разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем; - выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем.

– **владеть** – профессиональной терминологией в области информационной безопасности; – навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем; – методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем; – навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем; – навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем.

#### 4. Название разделов (тем) дисциплины

Названия разделов дисциплины
8 семестр
1 Поиск, изучение, обобщение и систематизация научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности.
2 Составление технического задания на автоматизированные информационные системы
3 Проектирование автоматизированных информационных систем
4 Основные стадии создания автоматизированных информационных систем
5 Содержание работ на этапах создания автоматизированных информационных систем
6 Средства автоматизации проектирования автоматизированных информационных систем
14 Составление технического задания на разработку автоматизированной системы
15 Проведение предпроектного исследования. Защита результатов научно-исследовательской работы
16 Реализация модуля безопасности системы
9 семестр
7 Средства построения пользовательского интерфейса
8 Средства разработки программноинформационного ядра информационных систем
9 Тестирование автоматизированных информационных систем

10 Подготовка приложения к распространению
11 Ввод в эксплуатацию автоматизированных информационных систем
12 Эксплуатация автоматизированных информационных систем
13 Анализ рисков информационной безопасности Автоматизированной системы