

## **Паспорт научной специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность»**

### **Область науки:**

2. Технические науки

### **Группа научных специальностей:**

2.3. Информационные технологии и телекоммуникации

### **Наименование отрасли науки, по которой присуждаются ученые степени:**

Технические

Физико-математические

### **Шифр научной специальности:**

2.3.6. Методы и системы защиты информации, информационная безопасность

### **Направления исследований:**

1. Теория и методология обеспечения информационной безопасности и защиты информации.
2. Методы, аппаратно-программные средства и организационные меры защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида.
3. Методы, модели и средства выявления, идентификации, классификации и анализа угроз нарушения информационной безопасности объектов различного вида и класса.
4. Системы документооборота (вне зависимости от степени их компьютеризации) и средства защиты циркулирующей в них информации.
5. Методы, модели и средства (комплексы средств) противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет.
6. Методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам в компьютерных сетях.
7. Модели и методы формирования комплексов средств противодействия угрозам информационной безопасности для различного вида объектов защиты (систем, цепей поставки) вне зависимости от области их функционирования.
8. Анализ рисков нарушения информационной безопасности и уязвимости процессов обработки, хранения и передачи информации в информационных системах любого вида и области применения.
9. Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем, позволяющие получать оценки показателей информационной безопасности.
10. Модели и методы оценки защищенности информации и информационной безопасности объекта.

11. Модели и методы оценки эффективности систем (комплексов), средств и мер обеспечения информационной безопасности объектов защиты.
12. Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа.
13. Методы и модели выявления и противодействия распространению ложной и вредоносной информации.
14. Мероприятия и механизмы формирования политики обеспечения информационной безопасности для объектов всех уровней иерархии системы управления.
15. Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.
16. Модели, методы и средства обеспечения аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности, и расследования инцидентов информационной безопасности в автоматизированных информационных системах.
17. Методы, модели и средства разработки безопасного программного обеспечения, выявления в нем дефектов безопасности, противодействия скрытым каналам передачи данных и выявления уязвимостей в компьютерных системах и сетях.
18. Модели и методы управления информационной безопасностью, непрерывным функционированием и восстановлением систем, противодействия отказам в обслуживании.
19. Исследования в области безопасности криптографических алгоритмов, криптографических примитивов, криптографических протоколов. Защита инфраструктуры обеспечения применения криптографических методов.

**Смежные специальности (в т.ч. в рамках группы научной специальности)<sup>1</sup>:**

- 1.2.4. Кибербезопасность
- 2.3.1. Системный анализ, управление и обработка информации
- 2.3.4. Управление в организационных системах
- 2.3.8. Информатика и информационные процессы

---

<sup>1</sup>Для рекомендации научных специальностей в создаваемых диссертационных советах