

УТВЕРЖДАЮ

Проректор по учебной работе

И.А. Кузнецова

28 мая 2024 г.



## ОПИСАНИЕ

**основной образовательной программы (ООП)**

**высшего образования по направлению подготовки**

**10.04.01 Информационная безопасность**

**Направленность (профиль):** Управление информационной безопасностью.

**прием 2023 год**

ООП реализуется в соответствии с федеральным государственным образовательным стандартом высшего образования – магистратура по направлению подготовки 10.04.01 Информационная безопасность, утвержденным приказом Министерства науки и высшего образования Российской Федерации от 26 ноября 2020 г. № 1455

- 1. Квалификация, присваиваемая выпускникам** – магистр.
- 2. Объем программы магистратуры** составляет 120 зачетных единиц.
- 3. ООП реализуется** в очной форме.
- 4. Срок получения образования по ООП:**  
**в очной форме обучения**, включая каникулы, предоставляемые после прохождения государственной итоговой аттестации, составляет 2 года.
- 5. При реализации ООП применяется** электронное обучение, дистанционные образовательные технологии.
- 6. Требования к уровню образования лиц, поступающих на обучение по ООП** – абитуриент должен иметь документ о высшем образовании и о квалификации.
- 7. Области профессиональной деятельности и сферы профессиональной деятельности, в которых выпускники, освоившие программу ООП, могут осуществлять профессиональную деятельность:**

06 Связь, информационные и коммуникационные технологии (в сфере защиты информации в компьютерных системах и сетях, автоматизированных системах).

**8. В рамках освоения ООП выпускники готовятся к решению задач профессиональной деятельности следующих типов:**

- проектный;
- научно-исследовательский;
- организационно-управленческий.

**9. Профессиональные задачи, которые готов решать выпускник, освоивший ООП:**

- разработка математических моделей систем обеспечения информационной безопасности, математическое доказательство их соответствия выбранным политикам безопасности;
- анализ математических моделей систем обеспечения информационной безопасности, тестирование средств защиты информации на соответствие этим моделям.

**10. Результаты освоения ООП.**

В результате освоения ООП у выпускника должны быть сформированы следующие компетенции:

**Универсальные компетенции (УК):**

УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, выработать стратегию действий.

УК-2. Способен управлять проектом на всех этапах его жизненного цикла;

УК-3. Способен организовывать и руководить работой команды, выработывая командную стратегию для достижения поставленной цели.

УК-4. Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия.

УК-5. Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия.

УК-6. Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки.

**Общепрофессиональные компетенции (ОПК):**

ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание.

ОПК-2. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности.

ОПК-3. Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности.

ОПК-4. Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок.

ОПК-5. Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи.

### **Профессиональные компетенции (ПК):**

ПК-1. Способен разрабатывать математические модели систем обеспечения информационной безопасности, математически доказывать их соответствие выбранным политикам безопасности.

ПК-2. Способен анализировать математические модели систем обеспечения информационной безопасности, а также проводить тестирование средств защиты информации на соответствие этим моделям.

**11. Формы проведения государственной итоговой аттестации:** защита выпускной квалификационной работы.