

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ  
Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Магнитогорский государственный технический университет им. Г.И. Носова»



УТВЕРЖДАЮ

Ректор ФГБОУ ВО «МГТУ им. Г.И. Носова»

В.М. Колокольцев

« 26 » апреля 20 17 г.

Номер внутривузовской регистрации

СП - АЦБ - 16

**ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ВЫСШЕГО ОБРАЗОВАНИЯ**

Специальность

**10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ  
АВТОМАТИЗИРОВАННЫХ СИСТЕМ**

Специализация программы

**ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ  
РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ**

Уровень высшего образования

**специалитет**

Форма обучения

**очная**

Программа одобрена Ученым советом «МГТУ им. Г.И. Носова»

Протокол № 4 « 26 » апреля 20 17 г.

Согласовано:

Директор института Энергетики и  
автоматизированных систем  
Заведующий кафедрой информатики и  
информационной безопасности,  
руководитель образовательной программы

С. И. Лукьянов

И. И. Баранкова

Магнитогорск, 2017

## **ПЕРЕЧЕНЬ ДОКУМЕНТОВ, ВКЛЮЧЕННЫХ В ОБРАЗОВАТЕЛЬНУЮ ПРОГРАММУ**

### **1 ОБЩАЯ ХАРАКТЕРИСТИКА ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ:**

- 1.1 Общие положения
- 1.2 Нормативные документы для разработки образовательной программы
- 1.3 Требования к уровню подготовки, необходимому для освоения ОП
- 1.4 Сроки, трудоемкость освоения образовательной программы

### **2 ХАРАКТЕРИСТИКА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ**

### **3 ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ**

### **4 ДОКУМЕНТЫ, РЕГЛАМЕНТИРУЮЩИЕ СОДЕРЖАНИЕ И ОРГАНИЗАЦИЮ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА:**

- 4.1 Учебный план, включая календарный учебный график
- 4.2 Рабочие программы дисциплин (модулей)
- 4.3 Программы практик и программа научно-исследовательской работы

### **5 РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ:**

- 5.1 Учебно-методическое и информационное обеспечение образовательной программы
- 5.2 Кадровое обеспечение образовательной программы
- 5.3 Материально-техническое обеспечение образовательной программы

### **6 ХАРАКТЕРИСТИКА СРЕДЫ ВУЗА, ОБЕСПЕЧИВАЮЩЕЙ РАЗВИТИЕ ОБЩЕКУЛЬТУРНЫХ И СОЦИАЛЬНО-ЛИЧНОСТНЫХ КОМПЕТЕНЦИЙ ВЫПУСКНИКОВ**

### **7 НОРМАТИВНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ СИСТЕМЫ ОЦЕНКИ КАЧЕСТВА ОСВОЕНИЯ ОБУЧАЮЩИМИСЯ ОП:**

- 7.1 Фонд оценочных средства для проведения промежуточной аттестации
- 7.2 Программа государственной итоговой аттестации

# **1 ОБЩАЯ ХАРАКТЕРИСТИКА ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ**

## **1.1 Общие положения**

Образовательная программа (ОП) представляет собой комплекс основных характеристик образования (объем, содержание, планируемые результаты), организационно-педагогических условий, форм аттестации, который представлен в виде общей характеристики образовательной программы, учебного плана, календарного учебного графика, рабочих программ дисциплин (модулей), программ практик, оценочных средств, методических материалов, и иных компонентов.

Целью образовательной программы по специальности 10.05.03 "Информационная безопасность автоматизированных систем" является формирование и развитие общекультурных, общепрофессиональных, профессиональных и профессионально-специализированных компетенций по видам профессиональной деятельности в области науки, техники и технологии, охватывающие совокупность проблем, связанных с обеспечением информационной безопасности автоматизированных систем в условиях существования угроз в информационной сфере, в соответствии с требованиями ФГОС ВО и специализацией ОП.

В области воспитания целью ОП является развитие у обучающихся личностных качеств, способствующих их творческой активности, общекультурному росту и социальной мобильности, умения работать индивидуально и в коллективе, ответственности, самостоятельности, гражданственности, приверженности этическим ценностям, целеустремленности и настойчивости в достижении целей.

В образовательной программе определяются:

- планируемые результаты освоения образовательной программы – компетенции обучающихся, установленные образовательным стандартом;
- планируемые результаты обучения по каждой дисциплине (модулю) и практике – знания, умения, навыки и (или) опыт деятельности, характеризующие этапы формирования компетенций и обеспечивающие достижение планируемых результатов освоения образовательной программы.

## **1.2 Нормативные документы для разработки образовательной программы**

Нормативную базу для разработки образовательной программы составляют:

- Федеральный закон Российской Федерации «Об образовании в Российской Федерации» от 29.12.2012 № 273-ФЗ.
- Порядок организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры», утвержденный приказом Министерства образования и науки Российской Федерации от 19.12.2013 № 1367.
- Федеральный государственный образовательный стандарт высшего образования по специальности 10.05.03 "Информационная безопасность автоматизированных систем", утвержденный приказом Министерства образования и науки Российской Федерации от 1 декабря 2016 г. № 1509
- Устав федерального государственного бюджетного образовательного учреждения высшего образования «Магнитогорский государственный технический университет им. Г.И. Носова».

### **1.3 Требования к уровню подготовки, необходимому для освоения образовательной программы**

К освоению программы специалитета допускаются лица, имеющие среднее общее образование.

Условия приема по образовательным программам специалитета регламентируются Правилами приёма в ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова».

### **1.4 Сроки, трудоемкость освоения образовательной программы**

Нормативный срок освоения образовательной программы для очной формы обучения составляет (включая каникулы, предоставляемые после прохождения государственной итоговой аттестации) 5 лет.

Общая трудоемкость освоения ОП составляет 300 ЗЕТ или 11128 часов.

Направленность (специализация) ОП – "Обеспечение информационной безопасности распределенных информационных систем".

## **2 ХАРАКТЕРИСТИКА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ**

В соответствии с ФГОС ВО область профессиональной деятельности выпускников, освоивших программу специалитета включает:

– сферы науки, техники и технологии, охватывающие совокупность проблем, связанных с обеспечением информационной безопасности автоматизированных систем в условиях существования угроз в информационной сфере.

Объектами профессиональной деятельности выпускников, освоивших программу специалитета, являются:

– автоматизированные системы, функционирующие в условиях существования угроз в информационной сфере и обладающие информационно-технологическими ресурсами, подлежащими защите;

– информационные технологии, формирующие информационную инфраструктуру в условиях существования угроз в информационной сфере и задействующие информационно-технологические ресурсы, подлежащие защите;

– технологии обеспечения информационной безопасности автоматизированных систем;

– системы управления информационной безопасностью автоматизированных систем.

Виды профессиональной деятельности, к которым готовятся выпускники, освоившие программу специалитета

- научно-исследовательская;
- проектно-конструкторская;
- контрольно-аналитическая;
- организационно-управленческая;
- эксплуатационная.

Выпускник, освоивший программу специалитета, готов решать следующие профессиональные задачи:

в соответствии с видами профессиональной деятельности:



– **научно-исследовательская деятельность:**

сбор, обработка, анализ и систематизация научно-технической информации по проблематике информационной безопасности автоматизированных систем;

подготовка научно-технических отчетов, обзоров, докладов, публикаций по результатам выполненных исследований;

моделирование и исследование свойств защищенных автоматизированных систем;

анализ защищенности информации в автоматизированных системах и безопасности реализуемых информационных технологий;

разработка эффективных решений по обеспечению информационной безопасности автоматизированных систем;

**проектно-конструкторская деятельность:**

сбор и анализ исходных данных для проектирования защищенных автоматизированных систем;

разработка политик информационной безопасности автоматизированных систем;

разработка защищенных автоматизированных систем в сфере профессиональной деятельности, обоснование выбора способов и средств защиты информационно-технологических ресурсов автоматизированных систем;

выполнение проектов по созданию программ, комплексов программ, программно-аппаратных средств, баз данных, компьютерных сетей для защищенных автоматизированных систем;

разработка систем управления информационной безопасностью автоматизированных систем;

**контрольно-аналитическая:**

контроль работоспособности и эффективности применяемых средств защиты информации;

выполнение экспериментально-исследовательских работ при сертификации средств защиты информации и аттестации автоматизированных систем;

проведение инструментального мониторинга защищенности автоматизированных систем и анализа его результатов;

**организационно-управленческая деятельность:**

организация работы коллектива, принятие управленческих решений в условиях спектра мнений, определение порядка выполнения работ;

организационно-методическое обеспечение информационной безопасности автоматизированных систем;

организация работ по созданию, внедрению, эксплуатации и сопровождению защищенных автоматизированных систем;

контроль реализации политики информационной безопасности;

**эксплуатационная деятельность:**

реализация информационных технологий в сфере профессиональной деятельности с использованием защищенных автоматизированных систем;

администрирование подсистем информационной безопасности автоматизированных систем;

мониторинг информационной безопасности автоматизированных систем;

управление информационной безопасностью автоматизированных систем;

обеспечение восстановления работоспособности систем защиты информации при возникновении нештатных ситуаций;

в соответствии со специализацией:

- разработка и исследование моделей информационно-технологических ресурсов, модели угроз и модели нарушителей информационной безопасности в распределенных информационных системах;
- удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах;
- аудит защищенности информационно-технологических ресурсов;
- координация деятельности подразделений и специалистов по защите информации в организациях, в том числе на предприятиях и в учреждениях;

### **3 ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ**

В результате освоения программы специалитета у выпускника должны быть сформированы общекультурные, общепрофессиональные, профессиональные и профессионально-специализированные компетенции.

Выпускник, освоивший программу специалитета, должен обладать следующими общекультурными компетенциями (ОК):

- способностью использовать основы философских знаний для формирования мировоззренческой позиции (ОК-1);
- способностью использовать основы экономических знаний в различных сферах деятельности (ОК-2);
- способностью анализировать основные этапы и закономерности исторического развития России, её место и роль в современном мире для формирования гражданской позиции и развития патриотизма (ОК-3);
- способностью использовать основы правовых знаний в различных сферах деятельности (ОК-4);
- способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5);
- способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6);
- способностью к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности (ОК-7);
- способностью к самоорганизации и самообразованию (ОК-8);
- способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности (ОК-9).

Выпускник, освоивший программу специалитета, должен обладать следующими общепрофессиональными компетенциями (ОПК):

- способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач (ОПК-1);
- способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математики

ческого анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники (ОПК-2);

– способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности (ОПК-3);

– способностью понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах (ОПК-4);

– способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-5);

– способностью применять нормативные правовые акты в профессиональной деятельности (ОПК-6);

– способностью применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций (ОПК-7);

– способностью к освоению новых образцов программных, технических средств и информационных технологий (ОПК-8).

Выпускник, освоивший программу специалитета, должен обладать профессиональными компетенциями, соответствующими виду (видам) профессиональной деятельности, на который (которые) ориентирована программа специалитета:

**научно-исследовательская деятельность:**

– способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке (ПК-1);

– способностью создавать и исследовать модели автоматизированных систем (ПК-2);

– способностью проводить анализ защищенности автоматизированных систем (ПК-3);

– способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-4);

– способностью проводить анализ рисков информационной безопасности автоматизированной системы (ПК-5);

– способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности (ПК-6);

– способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ (ПК-7);

**проектно-конструкторская деятельность:**

– способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем (ПК-8);

– способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-9);

– способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-10);

– способностью разрабатывать политику информационной безопасности автоматизированной системы (ПК-11);

– способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы (ПК-12);

– способностью участвовать в проектировании средств защиты информации автоматизированной Системы (ПК-13);

**контрольно-аналитическая деятельность:**

– способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-14);

– способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем (ПК-15);

– способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации (ПК-16);

– способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации (ПК-17);

**организационно-управленческая деятельность:**

– способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности (ПК-18);

– способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы (ПК-19);

– способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности (ПК-20);

– способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем (ПК-21);

– способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-22);

– способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа (ПК-23);

**эксплуатационная деятельность:**

– способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-24);

– способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций (ПК-25);

– способностью администрировать подсистему информационной безопасности автоматизированной системы (ПК-26);

– способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы (ПК-27);

– способностью управлять информационной безопасностью автоматизированной системы (ПК-28).

Выпускник, освоивший программу специалитета, должен обладать профессионально-специализированными компетенциями, соответствующими направленности (специали-



зации) программы "Обеспечение информационной безопасности распределенных информационных систем":

- способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах (ПСК-7.1);

- способностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах (ПСК-7.2);

- способностью проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем (ПСК-7.3);

- способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах (ПСК-7.4);

- способностью координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении (ПСК-7.5).

Матрица формирования компетенций с критериями их оценивания на этапах формирования прилагается.