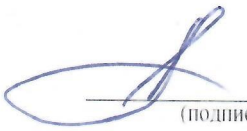
МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
«Санкт-Петербургский государственный университет
аэрокосмического приборостроения»

УТВЕРЖДАЮ
Руководитель направления 10.04.01
канд. техн. наук, доц.



_____ А.А. Овчинников
(подпись) (инициалы, фамилия)
«31» августа 2021 г.

ОБЩАЯ ХАРАКТЕРИСТИКА

образовательной программы высшего образования

Укрупненная группа подготовки: 10.00.00 Информационная безопасность

Уровень высшего образования: магистратура

Направление подготовки: 10.04.01 Информационная безопасность

Направленность (профиль): Интеллектуальные средства обеспечения безопасности объектов

Санкт-Петербург 2021

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Общие сведения об образовательной программе (ОП)

Образовательная программа по направлению 10.04.01 Информационная безопасность направленности «Интеллектуальные средства обеспечения безопасности объектов» разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 10.04.01 Информационная безопасность (зарегистрирован Минюстом России 18.02.2021, регистрационный №62549), а также государственными нормативными актами и локальными актами ГУАП.

Образовательная программа разработана с учетом профессиональных стандартов, соответствующих профессиональной деятельности выпускников, перечень которых приведен в Приложении 1.

Выпускнику, освоившему образовательную программу, присваивается квалификация: «магистр».

Обучение по образовательной программе осуществляется в очной форме. Срок обучения по очной форме - 2 года.

Объем образовательной программы - 120 зачетных единиц.

Язык, на котором осуществляется образовательная деятельность: русский.

1.2 Цель образовательной программы

Целью образовательной программы является формирование у выпускника:

- универсальных и общепрофессиональных компетенций в соответствии с ФГОС ВО;

- профессиональных компетенций, установленных ГУАП, на основе профессиональных стандартов, соответствующих профессиональной деятельности выпускников, а также на основе анализа требований к профессиональным компетенциям, предъявляемых к выпускникам на рынке труда, обобщения отечественного и зарубежного опыта, проведения консультаций с ведущими работодателями, объединениями работодателей отрасли, в которой востребованы выпускники, приведенных в разделе 2 настоящего документа.

1.3 Структура образовательной программы

Структура образовательной программы включает следующие блоки: Блок 1 "Дисциплины (модули)"; Блок 2 "Практика"; Блок 3 "Государственная итоговая аттестация".

В рамках образовательной программы выделяется обязательная часть, установленная ФГОС ВО, и часть, формируемая участниками образовательных отношений.

Объём контактной работы обучающихся с педагогическими работниками ГУАП при проведении учебных занятий по программе магистратуры составляет не менее 50 процентов.

2 ХАРАКТЕРИСТИКА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ ВЫПУСКНИКОВ

2.1 Общее описание профессиональной деятельности выпускников

Области профессиональной деятельности и сферы профессиональной деятельности, в которых выпускники, освоившие программу, могут осуществлять профессиональную деятельность:

- 06 Связь, информационные и коммуникационные технологии (в сферах: защиты информации в компьютерных системах и сетях, автоматизированных системах, системах и сетях электросвязи, технической защиты информации, защиты значимых объектов критической информационной инфраструктуры, информационно-аналитических систем безопасности);

- 40 Сквозные виды профессиональной деятельности.

Выпускники, освоившие образовательную программу, готовы решать задачи профессиональной деятельности следующих типов:

- проектный;

- научно-исследовательский;

- организационно-управленческий.

2.2 Перечень основных задач и объектов (или областей знаний) профессиональной деятельности (ПД) выпускников

Область ПД (по Реестру Минтруда)	**Типы задач ПД**	**Задачи ПД**	**Объекты ПД (или области знания)**
06 Связь, информационные и коммуникационные технологии (в сферах: защиты информации в компьютерных системах и сетях, автоматизированных системах, системах и сетях электросвязи, технической защиты информации, защиты значимых объектов критической информационной инфраструктуры, информационно-аналитических систем безопасности) 40 Сквозные виды деятельности	научно-исследовательский	анализ фундаментальных и прикладных проблем информационной безопасности в условиях становления современного информационного общества; разработка планов и программ проведения научных исследований и технических разработок, подготовка отдельных заданий для исполнителей; выполнение научных исследований с применением соответствующих физических и математических методов; подготовка по результатам научных исследований отчётов, статей, докладов на научных конференциях.	Фундаментальные и прикладные проблемы информационной безопасности; объекты информатизации, информационные ресурсы и информационные технологии, компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы; средства и технологии обеспечения информационной безопасности и защиты информации; методы и средства проектирования, моделирования и экспериментальной отработки систем, средств и технологий обеспечения информационной безопасности объектов информатизации; образовательный процесс в области информационной безопасности

06 Связь, информационные и коммуникационные технологии (в сферах: защиты информации в компьютерных системах и сетях, автоматизированных системах, системах и сетях электросвязи, технической защиты информации, защиты значимых объектов критической информационной инфраструктуры, информационно-аналитических систем безопасности)	проектный	системный анализ прикладной области, выявление угроз и оценка уязвимости информационных систем, разработка требований и критериев оценки информационной безопасности; обоснование выбора состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов; разработка систем, комплексов, средств и технологий обеспечения информационной безопасности; разработка программ и методик испытаний средств и систем обеспечения информационной безопасности	Фундаментальные и прикладные проблемы информационной безопасности; объекты информатизации, информационные ресурсы и информационные технологии, компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы; средства и технологии обеспечения информационной безопасности и защиты информации; экспертиза, сертификация и контроль защищённости информации и объектов информатизации; методы и средства проектирования, моделирования и экспериментальной отработки систем, средств и технологий обеспечения информационной безопасности объектов информатизации
06 Связь, информационные и коммуникационные технологии (в сферах: защиты информации в компьютерных системах и сетях, автоматизированных системах, системах и сетях электросвязи, технической защиты информации, защиты значимых объектов критической информационной инфраструктуры, информационно-аналитических систем безопасности)	организационно-управленческий	организация работы коллектива исполнителей, принятие управленческих решений, определения порядка выполнения работ; организация управления информационной безопасностью, организация работы по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности (ФСБ России), Федеральной службы по техническому и экспортному контролю (ФСТЭК России).	объекты информатизации, информационные ресурсы и информационные технологии, компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы; экспертиза, сертификация и контроль защищённости информации и объектов информатизации; организация и управление информационной безопасностью

3 ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОП

3.1 Универсальные компетенции выпускников и индикаторы их достижения (УК)

Категория (группа) УК	Код и наименование УК	Код и наименование индикатора достижения УК
Системное и критическое мышление	УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.З.1. знать методы критического анализа и системного подхода; методики разработки стратегии действий для выявления и решения проблемных ситуаций УК-1.З.2. знать цифровые ресурсы, инструменты и сервисы для решения задач/проблем профессиональной деятельности УК-1.У.1. уметь искать нужные источники информации; воспринимать, анализировать, сохранять и передавать информацию с использованием цифровых средств; вырабатывать стратегию действий для решения проблемной ситуации УК-1.В.1. владеть навыками системного и критического мышления; методиками постановки цели, определения способов ее достижения УК-1.В.2. владеть навыками использования алгоритмов и цифровых средств, предназначенных для анализа информации и данных
Разработка и реализация проектов	УК-2. Способен управлять проектом на всех этапах его жизненного цикла	УК-2.З.1. знать этапы жизненного цикла проекта; виды ресурсов и ограничений для решения проектных задач; необходимые для осуществления проектной деятельности правовые нормы и принципы управления проектами УК-2.З.2. знать цифровые инструменты, предназначенные для разработки проекта/решения задачи; методы и программные средства управления проектами УК-2.У.1. уметь определять целевые этапы, основные направления работ; объяснять цели и формулировать задачи, связанные с подготовкой и реализацией проекта УК-2.У.2. уметь выдвигать альтернативные варианты действий с целью выработки новых оптимальных алгоритмов действий по проекту УК-2.В.1. владеть навыками управления проектом на всех этапах его жизненного цикла УК-2.В.2. владеть навыками решения профессиональных задач в условиях цифровизации общества
Командная работа и лидерство	УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	УК-3.З.1. знать методики формирования команды; методы эффективного руководства коллективом; основные теории лидерства и стили руководства УК-3.З.2. знать цифровые средства, предназначенные для взаимодействия с другими людьми и выполнения командной работы УК-3.У.1. уметь вырабатывать командную стратегию для достижения поставленной цели; использовать цифровые средства, предназначенные для организации командной работы УК-3.В.1. владеть навыками организации командной работы; разрешения конфликтов и противоречий при деловом общении на основе учета интересов всех сторон УК-3.В.2. владеть навыками использования цифровых средств, обеспечивающих удаленное взаимодействие членов команды
Коммуникация	УК-4. Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академи-	УК-4.З.1. знать правила и закономерности личной и деловой устной и письменной коммуникации; современные коммуникативные технологии на русском и иностранном(ых) языке(ах) УК-4.З.2. знать современные технологии, обеспечивающие коммуникацию и кооперацию в цифровой среде

	ческого и профессионального взаимодействия	УК-4.У.1. уметь применять на практике технологии коммуникации и кооперации для академического и профессионального взаимодействия, в том числе в цифровой среде, для достижения поставленных целей УК-4.В.1. владеть навыками межличностного делового общения на русском и иностранном(ых) языке(ах) с применением современных технологий и цифровых средств коммуникации
Межкультурное взаимодействие	УК-5. Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	УК-5.З.1. знать правила и технологии эффективного межкультурного взаимодействия УК-5.У.1. уметь взаимодействовать с представителями иных культур с соблюдением этических и межкультурных норм УК-5.В.1. владеть навыками межкультурного взаимодействия при выполнении профессиональных задач
Самоорганизация и саморазвитие (в том числе здоровьесбережение)	УК-6. Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	УК-6.З.1. знать основные принципы профессионального и личностного развития с учетом особенностей цифровой экономики и требований рынка труда; способы совершенствования своей деятельности на основе самооценки и образования УК-6.У.1. уметь определять и реализовывать приоритеты совершенствования собственной деятельности на основе самооценки, в том числе с использованием цифровых средств; решать задачи собственного личностного и профессионального развития УК-6.В.1. владеть навыками решения задач самоорганизации и собственного личностного и профессионального развития на основе самооценки, самоконтроля, в том числе с использованием цифровых средств

3.2 Общепрофессиональные компетенции выпускников и индикаторы их достижения (ОПК)

Код и наименование ОПК	**Код и наименование индикатора достижения ОПК**	
ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;	ОПК-1.З.1	знать основы отечественных и зарубежных стандартов в области обеспечения информационной безопасности
	ОПК-1.З.2	знает направления развития и проблемы компьютерного моделирования сложных систем; направления развития технологий проектирования информационных, автоматизированных и автоматических систем
	ОПК-1.З.3	знает современную нормативную базу и ГОСТы, регламентирующие процесс разработки ТЗ. Правила, способы и методы организации совместных разработок.
	ОПК-1.З.4	знает методы проектирования и построения систем информационной безопасности, включая методы тестирования эффективности и оценки надёжности
	ОПК-1.У.1	уметь проектировать информационные системы с учетом различных технологий обеспечения информационной безопасности
	ОПК-1.У.2	умеет обосновывать и планировать состав и архитектуру моделируемых сложных систем; обосновывать и планировать состав и архитектуру проектируемых информационных, автоматизированных и автоматических систем

	ОПК-1.У.3	умеет формировать актуальную модель угроз для АИС и учитывать её положения при формировании требований ТЗ на проектируемую систему обеспечения ИБ
	ОПК-1.У.4	умеет разрабатывать и обосновывать критерии оценки эффективности проектируемой системы обеспечения ИБ. Оценивать эффективность решений и анализировать показатели деятельности
	ОПК-1.У.5	умеет обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности
	ОПК-1.В.1	владеть навыками участия в разработке системы обеспечения информационной безопасности объекта
	ОПК-1.В.2	владеет навыками разработки концептуальных стратегий решения задач моделирования и проектирования автоматизированных информационных систем и систем обеспечения ИБ
	ОПК-1.В.3	владеет навыками планирования и оценки трудоёмкости проекта, включая техническое, кадровое и финансовое обеспечение, принятие совместных решений
ОПК-2. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности;	ОПК-2.З.1	знает методы концептуального проектирования технологий обеспечения информационной безопасности
	ОПК-2.З.2	знает направления развития и проблемы компьютерного моделирования сложных систем; направления развития технологий проектирования информационных, автоматизированных и автоматических систем
	ОПК-2.З.3	знает современные методы и средства тестирования
	ОПК-2.З.4	знать принципы построения и функционирования современных информационных систем
	ОПК-2.З.5	знать назначение комплексной системы защиты информации, принципы ее организации и этапы разработки
	ОПК-2.З.6	знать требования к системам комплексной защиты информации
	ОПК-2.У.1	умеет выбирать и обосновывать преимущества методов решения задач для защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью
	ОПК-2.У.2	умеет разрабатывать тестовые планы и сценарии тестирования разработанного продукта
	ОПК-2.У.3	умеет управлять коллективом исполнителей и принимать управленческие решения
	ОПК-2.У.4	уметь проектировать подсистемы безопасности информационных систем с учетом действующих нормативных и методических документов
	ОПК-2.У.5	уметь разрабатывать модели угроз и нарушителей информационной безопасности информационных систем
	ОПК-2.В.1	владеет навыками выполнения работы по осуществлению при изготовлении, монтаже, наладке, испытаниях и сдаче в эксплуатацию систем и средств обеспечения информационной безопасности

	ОПК-2.В.2	владеет навыками практической реализации типовых задач разработки и исследования систем защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью
	ОПК-2.В.3	владеет средствами автоматизированного и ручного функционального тестирования
	ОПК-2.В.4	владеть навыками участия в организации комплексной системы защиты объекта
ОПК-3. Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности;	ОПК-3.З.1	знать основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, в области управления информационной безопасностью с целью разработки проектов организационно-распорядительных документов
	ОПК-3.З.2	знать правила создания технического задания на создание подсистем безопасности информационных систем
	ОПК-3.З.3	знать основные угрозы безопасности информации и модели нарушителя в информационных системах
	ОПК-3.З.4	знать основные нормативные правовые акты в области обеспечения информационной безопасности
	ОПК-3.З.5	знать нормативные методические документы ФСБ России в области защиты информации
	ОПК-3.З.6	знать нормативные методические документы ФСТЭК России в области информационной безопасности
	ОПК-3.У.1	уметь разрабатывать технические задания на создание подсистем обеспечения информационной безопасности
	ОПК-3.У.2	уметь проводить выбор, исследовать эффективность, проводить технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности
	ОПК-3.У.3	уметь разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации
	ОПК-3.У.4	уметь разрабатывать нормативно-методические материалы по регламентации системы организационной защиты информации
	ОПК-3.У.5	уметь разрабатывать организационно-распорядительную документацию по обеспечению информационной безопасности
	ОПК-3.У.6	уметь работать с технической и эксплуатационной документацией
	ОПК-3.У.7	уметь оценивать различные инструменты в области проектирования и управления информационной безопасности
	ОПК-3.В.1	владеть навыками разработки политик безопасности различных уровней
	ОПК-3.В.2	владеть навыками расчета и управления рисками информационной безопасности, навыками разработки положения о применимости механизмов контроля в контексте управления рисками информационной безопасности

	ОПК-3.В.3	владеть правилами построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, стоимости и сроков реализации
	ОПК-3.В.4	владеть навыками работы с нормативными правовыми актами в области 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-4.З.1	знать способы формулирования научной проблемы, гипотезы, выбора предмета, объекта, целей, задач исследования
	ОПК-4.З.2	знать основные принципы создания эскизного, технического, рабочего проектов
	ОПК-4.З.3	знать методы анализа и обоснования выбора решений по обеспечению требуемого уровня безопасности информационных систем
	ОПК-4.З.4	знать современные достижения науки в области информационной безопасности
	ОПК-4.З.5	знать правила, способы и методы организации, выполнения и представления результатов научного исследования
	ОПК-4.З.6	знать о правилах и стандартах разработки отчетной документации
	ОПК-4.З.7	знать основные категории и понятия информационно аналитической работы, принципы и методы ее ведения
	ОПК-4.З.8	знать методы выработки и принятия информационного решения
	ОПК-4.З.9	знать технологии поиска, изучения, обобщения и систематизации научной информации
	ОПК-4.З.10	знать виды отчетно-информационных документов, методы их подготовки
	ОПК-4.З.11	знать основные теоретико-числовые методы применительно к задачам защиты информации
	ОПК-4.У.1	уметь составлять пошаговый план научной деятельности, проводить предпроектные исследования
	ОПК-4.У.2	уметь работать с научной литературой, отбирать информацию по теме научного исследования, систематизировать, классифицировать полученную информацию
	ОПК-4.У.3	уметь определять комплекс мер для обеспечения безопасности информационных систем, составлять аналитические обзоры по вопросам обеспечения информационной безопасности систем
	ОПК-4.У.4	уметь использовать методы и средства анализа защищенности информационных систем
	ОПК-4.У.5	уметь использовать программные и аппаратные средства персонального компьютера для поиска и обработки информации
	ОПК-4.У.6	уметь разрабатывать планы и программы проведения научных исследований в соответствии с техническим заданием, ресурсным обеспечением и заданными сроками выполнения работы
	ОПК-4.У.7	уметь представлять результаты научно-исследовательской деятельности в виде презентаций, отчетов, устных докладов

	ОПК-4.У.8	уметь логически мыслить, вести научные дискуссии
	ОПК-4.У.9	уметь использовать справочную и научную литературу по тематике решаемых информационных задач, оценивать специальную информацию, систематизировать ее, принимать решение о ее дальнейшем использовании
	ОПК-4.В.1	владеть навыками структурирования информации по теме исследования
	ОПК-4.В.2	владеть навыками самостоятельного научного мышления, обобщения и систематизации информации
	ОПК-4.В.3	владеть навыками сбора и обработки информации в глобальной компьютерной сети, в том числе в мультидисциплинарных реферативных базах данных Scopus, Web of Knowledge
	ОПК-4.В.4	владеть методикой создания технического задания и технического проекта при организации НИОКР
	ОПК-4.В.5	владеть программными и программно-аппаратными средствами анализа систем защиты информации
	ОПК-4.В.6	владеть навыками поиска информации в глобальной информационной сети Интернет
	ОПК-4.В.7	владеть методологией научных исследований в сфере информационной безопасности
	ОПК-4.В.8	владеть навыками планирования научного исследования
	ОПК-4.В.9	владеть основными методами поиска и структурирования информации
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.	ОПК-5.3.1	знать теоретические и эмпирические методы научных исследований
	ОПК-5.3.2	знать порядок проведения научных исследований
	ОПК-5.3.3	знать методику проведения патентных исследований, объектом которых могут являться объекты техники, промышленной и интеллектуальной собственности (изобретения, полезные модели, программы для ЭВМ и базы данных и др.), ноу-хау и пр.
	ОПК-5.3.4	знает порядок организации процесса исследования эффективности системы управления ИБ
	ОПК-5.3.5	знать нормативные и методические материалы в сфере информационной безопасности
	ОПК-5.3.6	знать принципы организации технического, программного и информационного обеспечения информационной безопасности
	ОПК-5.3.7	знать методы построения оптимальных планов для научных экспериментов
	ОПК-5.3.8	знать правила, способы и методы организации, выполнения и представления результатов научного исследования
	ОПК-5.3.9	знать принципы построения и функционирования современных информационных систем
	ОПК-5.3.10	знать основные элементы научно-технического эксперимента

	ОПК-5.З.11	знать приемы выбора основных факторов эксперимента и технологию построения факторных планов
	ОПК-5.З.12	знать требования ГОСТов на оформление научно-технической документации
	ОПК-5.З.13	знать современные модели и методы измерения, прогнозирования, принятия решений при решении практических задач
	ОПК-5.З.14	знать принципы построения вероятностных моделей применительно к практическим задачам
	ОПК-5.У.1	уметь применять методы научных исследований в научной деятельности, в частности, при написании магистерской диссертации и научных статей
	ОПК-5.У.2	уметь составлять отчеты о патентных исследованиях по ГОСТ
	ОПК-5.У.3	умеет формализовать задачи анализа безопасности информационных систем, разрабатывать методики исследования и применять инструментальные средства анализа безопасности
	ОПК-5.У.4	уметь составлять и корректировать план проведения работ в зависимости от полученных результатов
	ОПК-5.У.5	уметь оформлять и представлять результаты, полученные в ходе выполнения научно-исследовательского проекта грамотно, лаконично, в достаточном объеме на русском и иностранном языках
	ОПК-5.У.6	уметь выбирать и применять в профессиональной деятельности экспериментальные и расчетно-теоретические методы исследований
	ОПК-5.У.7	уметь работать со специальными программным средствами для оформления проектной и отчетной документации
	ОПК-5.У.8	уметь обобщать полученные экспериментальные данные, анализировать и делать выводы
	ОПК-5.В.1	владеть навыками оформления научных публикаций в соответствие с шаблоном IEEE, требованиями научных конференций
	ОПК-5.В.2	владеть теоретическими и эмпирическими методами научного исследования при выполнении научно-исследовательских работ
	ОПК-5.В.3	владеть методикой оформления отчетов по научно-исследовательским работам согласно ГОСТ
	ОПК-5.В.4	владеет навыками выбора и обоснования критериев оценки защищенности открытых информационных систем
	ОПК-5.В.5	владеет навыками обработки, оценки и представления результатов исследования эффективности решений по управлению информационной безопасностью
	ОПК-5.В.6	владеть навыками разработки технической документации в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации
	ОПК-5.В.7	владеть навыками анализа получаемых результатов и формулировки выводов

	ОПК-5.В.8	владеть навыками формирования и аргументированного обоснования собственной позиции по различным проблемам защиты информации
	ОПК-5.В.9	владеть навыками представления результатов работы в виде презентаций, пояснительных записок, научных докладов и статей
	ОПК-5.В.10	владеть навыками самостоятельной работы, самоорганизации

3.3 Профессиональные компетенции (ПК) выпускников и индикаторы их достижения на основе профессиональных стандартов (ПС) (обобщенных трудовых функций (ОТФ)/трудовых функций (ТФ)), анализа опыта и пр.:

Задача ПД	**Объект или область знания**	**Код и наименование ПК**	**Код и наименование индикатора достижения ПК**	**Основание (ПС(ТФ/ОТФ), анализ опыта)**
Тип задач профессиональной деятельности: научно-исследовательский				
анализ фундаментальных и прикладных проблем информационной безопасности в условиях становления современного информационного общества; разработка планов и программ проведения научных исследований и технических разработок, подготовка отдельных заданий для исполнителей; выполнение научных исследований с применением соответствующих физических и математических методов; подготовка по результатам научных исследований отчётов, статей, докладов на научных конференциях.	Фундаментальные и прикладные проблемы информационной безопасности; объекты информатизации, информационные ресурсы и информационные технологии, компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы; средства и технологии обеспечения информационной безопасности и защиты информации; методы и средства проектирования, моделирования и экспериментальной отработки систем, средств и технологий обеспечения информационной безопасности объектов информатизации; образовательный процесс в области информационной безопасности	ПК-1. Способен оценивать уровень безопасности компьютерных систем и сетей	ПК-1.З.1. знает уязвимости компьютерных систем и сетей ПК-1.У.1 умеет анализировать компьютерную систему с целью определения уровня защищенности и доверия ПК-1.В.1. владеет оценкой рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем	06.032 (ТФ С/03.7)
анализ фундаментальных и прикладных проблем информационной безопасности в условиях становления современного информационного общества; разработка планов и программ проведения научных исследований и технических разработок, подго-	Фундаментальные и прикладные проблемы информационной безопасности; объекты информатизации, информационные ресурсы и информационные технологии, компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы; средства и технологии обеспечения ин-	ПК-2. Способен обосновывать перспективы проведения исследований в соответствующей области знаний	ПК-2.З.1. знает методы, средства и практику планирования, организации, проведения и внедрения научных исследований и опытно-конструкторских разработок ПК-2.У.1. умеет анализировать новую научную проблематику соответствующей области знаний	40.011 (ТФ D/01.7)

товка отдельных заданий для исполнителей; выполнение научных исследований с применением соответствующих физических и математических методов; подготовка по результатам научных исследований отчётов, статей, докладов на научных конференциях.	формационной безопасности и защиты информации; методы и средства проектирования, моделирования и экспериментальной отработки систем, средств и технологий обеспечения информационной безопасности объектов информатизации; образовательный процесс в области информационной безопасности		ПК-2.В.1. владеет навыками проведения анализа новых направлений исследований в соответствующей области знаний	
анализ фундаментальных и прикладных проблем информационной безопасности в условиях становления современного информационного общества; разработка планов и программ проведения научных исследований и технических разработок, подготовка отдельных заданий для исполнителей; выполнение научных исследований с применением соответствующих физических и математических методов; подготовка по результатам научных исследований отчётов, статей, докладов на научных конференциях.	Фундаментальные и прикладные проблемы информационной безопасности; объекты информатизации, информационные ресурсы и информационные технологии, компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы; средства и технологии обеспечения информационной безопасности и защиты информации; методы и средства проектирования, моделирования и экспериментальной отработки систем, средств и технологий обеспечения информационной безопасности объектов информатизации; образовательный процесс в области информационной безопасности	ПК-3. Способен проводить научно-исследовательские и опытно-конструкторские работы в сфере создания защищённых телекоммуникационных систем	ПК-3.З.1. знает национальные, межгосударственные и международные стандарты, устанавливающие требования к организации и проведению научно-исследовательских, опытно-конструкторских работ, опытной эксплуатации средств и систем защиты электросетей ПК-3.У.1. умеет планировать этапы выполнения НИОКР по созданию средств и систем защиты электросетей ПК-3.В.1. владеет организацией подготовки отчетных документов по итогам проведения НИОКР в соответствии с нормативными документами и требованиями заказчика	06.030 (ТФ D/03.7)
Тип задач профессиональной деятельности: проектный				
системный анализ прикладной области, выявление угроз и оценка уязвимости информационных систем, разработка требований и критериев оценки информационной безопасности; обоснование выбора состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов; разработка систем,	Фундаментальные и прикладные проблемы информационной безопасности; объекты информатизации, информационные ресурсы и информационные технологии, компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы; средства и технологии обеспечения информационной безопасности и защиты информации; экспертиза, сертификация и контроль защищённости информации и объектов информатизации; методы и средства проектирова-	ПК-4. Способен разрабатывать средства и системы защиты сетей электросвязи от несанкционированного доступа, а также защищённых телекоммуникационных систем	ПК-4.З.1. знает методы, способы, средства, последовательность и содержание этапов разработки средств и систем защиты сетей от НСД, защищённых телекоммуникационных систем ПК-4.У.1. умеет разрабатывать проекты, технические задания, планы и графики проведения работ по защите сетей от НСД и необходимую техническую документацию ПК-4.В.1. владеет разработкой предложений и практической реализацией элементов,	06.030 (ТФ D/02.7)

комплексов, средств и технологий обеспечения информационной безопасности; разработка программ и методик испытаний средств и систем обеспечения информационной безопасности	ния, моделирования и экспериментальной отработки систем, средств и технологий обеспечения информационной безопасности объектов информатизации		средств и систем защиты сетей от НСД, а также защищённых телекоммуникационных систем, включая разработку программного обеспечения	
системный анализ прикладной области, выявление угроз и оценка уязвимости информационных систем, разработка требований и критериев оценки информационной безопасности; обоснование выбора состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов; разработка систем, комплексов, средств и технологий обеспечения информационной безопасности; разработка программ и методик испытаний средств и систем обеспечения информационной безопасности	Фундаментальные и прикладные проблемы информационной безопасности; объекты информатизации, информационные ресурсы и информационные технологии, компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы; средства и технологии обеспечения информационной безопасности и защиты информации; экспертиза, сертификация и контроль защищённости информации и объектов информатизации; методы и средства проектирования, моделирования и экспериментальной отработки систем, средств и технологий обеспечения информационной безопасности объектов информатизации	ПК-5. Способен разрабатывать требования по защите и формировать политики безопасности компьютерных систем и сетей	ПК-5.З.1. знает виды политик безопасности компьютерных систем и сетей ПК-5.У.1. умеет формулировать задания по безопасности компьютерных систем ПК-5.В.1. владеет разработкой профилей защиты и заданий по безопасности	06.032 (ТФ С/02.7)
Тип задач профессиональной деятельности: организационно-управленческий				
организация работы коллектива исполнителей, принятие управленческих решений, определения порядка выполнения работ; организация управления информационной безопасностью, организация работы по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с нормативными правовыми актами и нормативными методическими	объекты информатизации, информационные ресурсы и информационные технологии, компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы; экспертиза, сертификация и контроль защищённости информации и объектов информатизации; организация и управление информационной безопасностью	ПК-6. Способен проводить контрольные проверки работоспособности и эффективности применяемых средств защиты информации	ПК-6.З.1. знает методы и методики оценки безопасности программно-аппаратных средств защиты информации ПК-6.У.1. умеет применять разработанные методики оценки защищенности программно-аппаратных средств защиты информации ПК-6.В.1. владеет оценкой работоспособности и эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик	06.032 (ТФ С/01.7)

документами Федеральной службы безопасности (ФСБ России), Федеральной службы по техническому и экспортному контролю (ФСТЭК России).				
организация работы коллектива исполнителей, принятие управленческих решений, определения порядка выполнения работ; организация управления информационной безопасностью, организация работы по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности (ФСБ России), Федеральной службы по техническому и экспортному контролю (ФСТЭК России).	объекты информатизации, информационные ресурсы и информационные технологии, компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы; экспертиза, сертификация и контроль защищённости информации и объектов информатизации; организация и управление информационной безопасностью	ПК-7. Способен проводить анализ угроз информационной безопасности в сетях электросвязи	ПК-7.З.1. знает организационно-технические мероприятия по обеспечению защиты сетей электросвязи от НСД и их эффективность ПК-7.У.1. умеет проводить проверку работоспособности и эффективности применяемых программно-аппаратных (в том числе криптографических) и технических средств защиты сетей электросвязи от НСД ПК-7.В.1. владеет выработкой предложений по предотвращению и нейтрализации угроз НСД к сетям электросвязи	06.030 (ТФ D/01.7)

4 ХАРАКТЕРИСТИКА РЕСУРСНОГО ОБЕСПЕЧЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

4.1 Общесистемное обеспечение реализации образовательной программы

4.1.1 ГУАП располагает на праве собственности или ином законном основании материально-техническим обеспечением образовательной деятельности (помещениями и оборудованием) для реализации образовательной программы в соответствии с учебным планом. Материально-техническое обеспечения, в том числе специализированное оборудование и лаборатории, указанные во ФГОС (при наличии), указывается в рабочих программах дисциплин (модулей), программах практик и программе ГИА.

4.1.2. Каждый обучающийся в течение всего периода обучения обеспечивается индивидуальным неограниченным доступом к электронной информационно-образовательной среде «pro.guap.ru» (далее – ЭОС ГУАП) из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»), как на территории ГУАП, так и вне ее.

4.1.3 При реализации образовательной программы возможно применение электронного обучения и/или дистанционных образовательных технологий.

4.1.4 Реализация ОП в сетевой форме не предусмотрена.

4.1.5 При реализации программы магистратуры в ГУАП определена кафедра Безопасности информационных систем, деятельность которой направлена на реализацию образовательных программ высшего образования по специальностям и направлениям подготовки, входящим в укрупнённую группу специальностей и направлений подготовки 10.00.00 «Информационная безопасность».

4.2 Материально-техническое и учебно-методическое обеспечение ОП

4.2.1 Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных ОП, оснащенные оборудованием и техническими средствами обучения, перечень и состав которых определяется в рабочих программах дисциплин (модулей), программах практик. Допускается частичная замена оборудования его виртуальными аналогами.

Для реализации программы магистратуры специально оборудованные помещения для проведения учебных занятий включают в себя:

лабораторию в области технологий обеспечения информационной безопасности и защищённых информационных систем;

аудиторию (защищаемое помещение) для проведения учебных занятий, в ходе которых до обучающихся доводится информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну;

специальную библиотеку (библиотеку литературы ограниченного доступа), предназначенную для хранения и обеспечения использования в образовательном процессе нормативных и методических документов ограниченного доступа.

Перечень помещений для самостоятельной работы обучающихся, оснащенных компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в ЭОС ГУАП, указывается в рабочих программах дисциплин (модулей).

4.2.2 ГУАП обеспечен необходимым комплектом лицензионного и (или) свободно распространяемого программного обеспечения, в том числе отечественного производства (состав определяется в рабочих программах дисциплин (модулей) и подлежит обновлению при необходимости).

4.2.3 При использовании в образовательном процессе печатных изданий библиотечный фонд укомплектован печатными изданиями из расчета не менее 0,25 экземпляра каждого из изданий, указанных в рабочих программах дисциплин (модулей), практик, на одного обучающегося из числа лиц, одновременно осваивающих соответствующую дисциплину (модуль), проходящих соответствующую практику.

4.2.4 Обучающимся обеспечен доступ (удаленный доступ), в том числе в случае применения электронного обучения, дистанционных образовательных технологий, к современным профессиональным базам данных и информационным справочным системам, в том числе электронно-библиотечным системам, состав которых определяется в рабочих программах дисциплин (модулей) и подлежит обновлению (при необходимости).

4.3 Кадровое обеспечение реализации ОП

4.3.1 Реализация ОП обеспечивается научно-педагогическими работниками ГУАП (НПР ГУАП), а также лицами, привлекаемыми ГУАП к реализации ОП на иных условиях.

4.3.2 Квалификация научно-педагогических работников отвечает квалификационным требованиям, указанным в квалификационных справочниках и (или) профессиональных стандартах (при наличии).

4.3.2 Не менее 80 процентов численности научно-педагогических работников, участвующих в реализации ОП, и лиц, привлекаемых к реализации ОП на иных условиях (исходя из количества замещаемых ставок, приведенного к целочисленным значениям), ведут научную, учебно-методическую и (или) практическую работу, соответствующую профилю преподаваемой дисциплины (модуля).

4.3.3 Не менее 5 процентов численности научно-педагогических работников ГУАП, участвующих в реализации ОП, и лиц, привлекаемых ГУАП к реализации ОП на иных условиях (исходя из количества замещаемых ставок, приведенного к целочисленным значениям),

является руководителями и (или) работниками иных организаций, осуществляющими трудовую деятельность в профессиональной сфере, соответствующей профессиональной деятельности, к которой готовятся выпускники (иметь стаж работы в данной профессиональной сфере не менее 3 лет).

4.3.4 Доля педагогических работников ГУАП (исходя из количества замещаемых ставок, приведенного к целочисленным значениям) составляет не менее 55 процентов от общего количества лиц, привлекаемых к реализации программы магистратуры.

4.3.5 Не менее 60 процентов численности научно-педагогических работников и лиц, привлекаемых к образовательной деятельности на иных условиях (исходя из количества замещаемых ставок, приведенного к целочисленным значениям), имеют ученую степень (в том числе ученую степень, полученную в иностранном государстве и признаваемую в Российской Федерации) и (или) ученое звание (в том числе ученое звание, полученное в иностранном государстве и признаваемое в Российской Федерации).

В реализации программы магистратуры принимает участие минимум один педагогический работник ГУАП, имеющий учёную степень по научной специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность».

4.4 Оценка качества подготовки обучающихся по ОП

Оценка качества освоения образовательной программы включает текущий контроль успеваемости, промежуточную аттестацию обучающихся и государственную итоговую аттестацию выпускников. Конкретные формы промежуточной аттестации обучающихся определяются учебным планом.

5 ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ ОБ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ

В распоряжении кафедры Безопасности информационных систем ГУАП находятся научно-исследовательские лаборатории:

- лаборатория программно-аппаратных средств защиты информации,
- лаборатория по корпоративной защите от внутренних угроз информационной безопасности,
- лаборатория игровых систем Интернета вещей.

Участие студентов в научно-исследовательской работе способствует углублению получаемых ими знаний, позволяет привлекать их к работам по заказам отечественных и зарубежных фирм.

В ходе обучения студенты проходят производственную практику в ведущих российских и зарубежных компаниях-партнерах, таких как ПАО «Интелтех», ООО «Люксофт Профешнл», ООО «Селектел», ООО «СевенТест», ФГУП «ГлавНИИВЦ», ООО «Санкт-Петербургский Центр разработок ЕМС», ООО «Необит», ООО «Инженерно-метрологическая лаборатория», ФГБУ «НМИЦ им. В.А. Алмазова», АО «Окенит», Комитет по информатизации и связи Правительства СПб, ООО «Нокиа Солюшнз энд Нетворкс», ООО «Хуавэй» и др., а выпускники кафедры имеют исключительные перспективы по трудоустройству в этих компаниях.

Потенциальные работодатели для выпускников образовательной программы:

1. Группа компаний InfoWatch
2. Комитет по информатизации и связи Правительства Санкт-Петербурга;
3. Компания «Доктор Веб»
4. АО «Лаборатория Касперского»
5. Министерство обороны РФ;
6. АО «НИИ «Рубин»;
7. ОАО «Информационные Технологии и Коммуникационные Системы» (ОАО «ИнфоТеКС»)
8. ООО "Газпромнефть-Нефтесервис"
9. ООО "Т-Системс РУС"
10. ООО «Газинформсервис»
11. ООО «Газпром энергохолдинг»;
12. ООО «Индустрия-А»
13. ООО «Интермедиа»
14. ООО «Код безопасности»
15. ООО «Лаборатория Интернета Вещей»

16. ООО «Люксофт Профешнл»

17. ООО «Научно-технический центр СевенТест»

18. ООО «НеоБит»

19. ООО «Нокиа Солюшнз энд Нетворкс»

20. ООО «Про-АдминИТи групп»

21. ООО «Пятый элемент»

22. ООО «Рэйдикс»

23. ООО «Санкт-Петербургский центр разработок ЕМС»

24. ООО «Селектел»

25. ООО «Хуавэй»

26. ООО «Яндекс»

27. ПАО «МегаФон»

28. ПАО «Ростелеком»

29. ПАО «Сбербанк России»;

30. ФГБУ Санкт-Петербургский институт информатики и автоматизации Российской академии наук

31. ФГУП «Центральный научно-исследовательский институт связи»

32. АО «НИИ телевидения»

33. АО «НПО «Эшелон»

34. АО Всероссийский научно-исследовательский институт радиоаппаратуры» (АО «ВНИИРА»)

35. Главное управление Министерства внутренних дел Российской Федерации по г. Санкт-Петербургу и Ленинградской области;

36. Государственная корпорация по космической деятельности «Роскосмос»

37. Федеральная служба безопасности Российской Федерации

38. ФСТЭК России

Ответственный за ОП ВО

заведующий кафедрой 51 _____ А.А. Овчинников

(должность, уч. степень) (подпись) (ФИО)

Приложение 1

Перечень профессиональных стандартов, соответствующих профессиональной деятельности выпускников

N п/п	Код ПС	Наименование области профессиональной деятельности. Наименование профессионального стандарта
06 Связь, информационные и коммуникационные технологии		
1.	06.030	Профессиональный стандарт «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. № 608н (зарегистрирован Министерством юстиции Российской Федерации 25 ноября 2016 г. № 44449).
2.	06.032	Профессиональный стандарт «Специалист по безопасности компьютерных систем и сетей», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 598н (зарегистрирован Министерством юстиции Российской Федерации 28 ноября 2016 г. № 44464).
40 Сквозные виды деятельности		
3.	40.011	Профессиональный стандарт «Специалист по научно-исследовательским и опытно-конструкторским разработкам», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 4 марта 2014 г. N 121н (зарегистрирован Министерством юстиции Российской Федерации 21 марта 2014 г. № 31692)