Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Гаврилов Сергей Александрович
Должность: И.О. Ректора
Дата подписания: 02.12.2025 14:48:03
Уникальный программный ключ:
f17218015d82e3c1457d1df9e244def505047355

МИНОБРНАУКИ РОССИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский университет
«МОСКОВСКИЙ ИНСТИТУТ ЭЛЕКТРОННОЙ ТЕХНИКИ»

УТВЕРЖДАЮ
Ректор _____С.А.Гаврилов
«02» 10 2025 года

ПРОГРАММА АСПИРАНТУРЫ

по научной специальности
2.3.6. «Методы и системы защиты информации, информационная безопасность»

Форма обучения – очная
Нормативный срок освоения программы – 3 года

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат 00FCD5F6E07DC83F809D56CE1D350ACCD1
Владелец ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ "МОСКОВСКИЙ ИНСТИТУТ ЭЛЕКТРОННОЙ ТЕХНИКИ"
Действителен с 09.04.2025 по 03.07.2026

Москва 2025 г.

1. Общие положения

1.1. Программа аспирантуры по научной специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность» – программа подготовки научных и научно-педагогических кадров в аспирантуре (далее – программа аспирантуры), реализуемая федеральным государственным автономным образовательным учреждением высшего профессионального образования «Национальный исследовательский университет «Московский институт электронной техники» (далее – МИЭТ, НИУ МИЭТ), разработана и утверждена на основании следующих нормативных документов:

- Федерального закона от 29.12.2012 г. № 273-ФЗ "Об образовании в Российской Федерации";
- Положения о присуждении ученых степеней из Постановления Правительства Российской Федерации от 24.09.2013 г. № 842 "О порядке присуждения ученых степеней";
- Федеральных государственных требований, Приказ Министерства науки и высшего образования Российской Федерации от 20.10.2021 г. № 951 «Об утверждении федеральных государственных требований к структуре программ подготовки научных и научно-педагогических кадров в аспирантуре…»;
- Постановления правительства Российской Федерации от 30.11.2021 г. № 2122 "Об утверждении Положения о подготовке научных и научно-педагогических кадров в аспирантуре (адъюнктуре)";
- Приказ Министерства науки и высшего образования Российской Федерации от 24.08.2021 г. № 786 "Об установлении соответствия направлений подготовки научно-педагогических кадров в аспирантуре научным специальностям…";
- паспорта научной специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность».

1.2. Цель освоения программы аспирантуры – выполнение индивидуального плана научной деятельности; написание, оформление и представление диссертации на соискание ученой степени кандидата наук к защите, содержащую решение научной задачи, имеющей значение для развития технической отрасли науки.

Основными задачами программы аспирантуры являются обеспечение:

- условий для осуществления аспирантами научной и научно-исследовательской деятельности в целях подготовки диссертации, в том числе, доступ к информации о научных и научно-технических результатах по научным тематикам, соответствующим научной специальности, по которой реализуется программа аспирантуры, доступ к научно-исследовательской и опытно-экспериментальной базе, необходимой для проведения научной (научно-исследовательской) деятельности в рамках подготовки диссертации;
- условий для подготовки аспиранта к сдаче кандидатских экзаменов;
- проведения учебных занятий по дисциплинам (модулям);
- условий для прохождения аспирантами педагогической практики;
- проведения контроля качества освоения программы аспирантуры посредством текущего контроля успеваемости, промежуточной и итоговой аттестации аспирантов.

При реализации программы аспирантуры НИУ МИЭТ возможно применение электронного обучения и дистанционных образовательных технологий.

Процесс обучения предполагает существенную долю самостоятельной работы аспиранта, регулярное взаимодействие с научным руководителем. Одной из технологий обучения по программе аспирантуры может быть включение аспирантов в исследовательские проекты НИУ МИЭТ, в том числе на условиях трудового договора.

Срок получения образования по программе аспирантуры по научной специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность» по очной форме обучения составляет 3 года.

При освоении программы аспирантуры инвалидами и лицами с ограниченными возможностями здоровья срок освоения программы аспирантуры может быть продлен не более чем на один год и составляет 4 года.

В аспирантуру по научной специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность» принимаются граждане, имеющие высшее образование уровня специалист или магистр, по соответствующей группе научных специальностей.

Направления диссертационных 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 при деструктивных воздействиях, направленных на данные и системы управления.
3. Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности и устойчивости управления.
4. Системы документооборота (вне зависимости от степени их компьютеризации) и средства зашиты циркулирующей в них информации.
5. Методы защиты информации в системах искусственного интеллекта и технологиях больших данных.
6. Методы и средства (комплексы средств) предупреждения, обнаружения и противодействия угрозам нарушения информационной безопасности и устойчивости управления, в открытых компьютерных сетях, включая Интернет, и связанных с ними систем.
7. Модели и методы формирования комплексов средств противодействия угрозам хищения (разрушения, модификации) информации и нарушения информационной безопасности для различного вида объектов защиты вне зависимости от области их функционирования.
8. Анализ рисков нарушения информационной безопасности и уязвимости процессов переработки информации в информационных системах любого вида и любых областях применения, управление рисками.
9. Модели, методы и средства активного противодействия и предотвращения различных деструктивных воздействия путем адаптивного интеллектуального управления информационной безопасностью и средствами защиты информации.
10. Модели и методы оценки защищенности информации и информационной безопасности объекта, модели угроз и модели нарушителя при различных видах деструктивного воздействия на данные и системы управления.
11. Модели и методы оценки эффективности систем (комплексов) обеспечения информационной безопасности объектов защиты, в том числе систем управления технологическими процессами.
12. Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа.
13. Мероприятия и механизмы формирования политики обеспечения информационной безопасности для объектов всех уровней иерархии системы управления объектами цифровизации различного назначения.
14. Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств обеспечения информационной безопасности и устойчивости управления объектами цифровизации.
15. Модели, методы и средства обеспечения внутреннего аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности, и расследования инцидентов нарушений безопасности информации и устойчивости управления объектов цифровизации.
16. Методы, модели и средства выявления недекларированных возможностей программного обеспечения и технических средств. Противодействие скрытым каналам передачи данных. Выявление уязвимостей в системах различного типа.
17. Модели и методы управления информационной безопасностью. Исследование устойчивости функционирования систем обеспечения информационной безопасности и защиты информации (в том числе с использованием методов искусственного интеллекта) к разнообразным деструктивным воздействиям в распределённых системах обработки данных и управления.
18. Исследования в области криптографии, алгоритмы и методы криптографической защиты информации, в том числе основанные на новых физических принципах, квантовая криптография.

19. Информационная безопасность социотехнических систем. Идентификация деструктивного информационного воздействия в социальных сетях.

20. Методы, организационные меры и технические средства защиты информации от утечки по техническим каналам.

21. Методы, методики и средства (комплексы) проведения специальных исследований технических средств. Методы, методики и средства (комплексы) контроля эффективности защиты информации от утечки по техническим каналам.

Виды профессиональной деятельности, к которым готовятся выпускники, освоившие программу аспирантуры:

- научная и научно-исследовательская деятельность в области информационной безопасности, направленная на обеспечение безопасности различных видов информации;
- преподавательская деятельность по образовательным программам высшего образования.

1.3. Планируемые результаты освоения программы аспирантуры

В результате освоения программы аспирантуры выпускник должен обладать следующими профессиональными компетенциями в рамках направления подготовки:

- способностью к самостоятельному проведению научных исследований и получению научных результатов, удовлетворяющих установленным требованиям к содержанию диссертации на соискание ученой степени кандидата наук по соответствующей научной специальности;
- способностью овладеть методологией научных исследований, включая представление полученных результатов, удовлетворяющих установленным требованиям к содержанию диссертации на соискание ученой степени кандидата наук;
- способностью к самостоятельному проведению научных исследований и получению научных результатов в области информационной безопасности;
- способностью преподавать и разрабатывать научно-методическое обеспечение учебных дисциплин в области информационной безопасности по программам бакалавриата и магистратуры;
- способностью овладеть технологией разработки учебно-методического обеспечения образовательного процесса высшей школы;
- готовностью к преподавательской деятельности в области информационной безопасности;
- способностью организовать контроль и оценку эффективности защиты информации;
- способностью проводить исследования основных характеристик средств защиты информации.

2. Общая характеристика программы аспирантуры

2.1. Программа аспирантуры предусматривает:

- научную и научно-исследовательскую деятельность и подготовку диссертации на соискание ученой степени кандидата наук;
- подготовку публикаций по результатам научной и научно-исследовательской деятельности;
- проведение учебных занятий по дисциплинам в форме лекций, научно-практических семинаров, круглых столов, видеоконференций и иных форм, в том числе и с использованием дистанционных образовательных технологий (ДОТ);
- подготовку и сдачу кандидатских экзаменов;
- проведение практической подготовки в форме педагогической практики;
- проведение контроля качества освоения программы аспирантуры посредством текущего контроля успеваемости, промежуточной аттестации обучающихся и государственной итоговой аттестации обучающихся.

2.2. Структура и содержание программы аспирантуры.

2.2.1. Программа аспирантуры включает в себя научный компонент, образовательный компонент, а также итоговую аттестацию.

Научный компонент программы аспирантуры включает:

- научную деятельность аспиранта, направленную на подготовку диссертации на соискание научной степени кандидата наук (далее – диссертация) к защите;

- подготовку публикаций, в которых излагаются основные научные результаты диссертации, в том числе в рецензируемых и в приравненных к ним научных изданиях;

- промежуточную аттестацию по этапам выполнения научного исследования.

Образовательный компонент программы аспирантуры включает дисциплины и педагогическую практику, а также промежуточную аттестацию по указанным дисциплинам и практике.

Итоговая аттестация по программам аспирантуры проводится в форме оценки диссертации на предмет ее соответствия критериям, установленным в Постановлении Правительства РФ от 24.09.2013 г. № 842 "О порядке присуждения ученых степеней".

2.2.2. Примерный план научно-исследовательской деятельности и подготовки диссертации для аспирантов (Приложение 1).

2.2.3. Содержание и реализация образовательного процесса по программе аспирантуры определяются следующими документами:

– Учебный план и календарный учебный график подготовки аспирантов по научной специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность»

– Программа научной деятельности

– Рабочая программа дисциплины «История и философия науки»

– Программа кандидатского экзамена по Истории и философии науки

– Рабочая программа дисциплины «Иностранный язык»

– Программа кандидатского экзамена по Иностранному языку

– Рабочая программа дисциплины «Методы и средства контроля эффективности защиты информации»

– Программа кандидатского экзамена по научной специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность»

– Рабочая программа дисциплины «Методология научного исследования и апробация результатов. Структура и содержание диссертации». Дополнительные модули по выбору:

Модуль 1. Научная коммуникация: теории и практика подготовки академического текста.

Модуль 2. Основы использования нейросетей и ИИ при подготовке канд.диссертации.

Модуль 3. Использование нейросетей в научных исследованиях при обработке больших объемов данных.

– Рабочая программа дисциплины «Управление информационной безопасностью».

– Рабочая программа дисциплины «Педагогика и психология высшего образования».

– Рабочая программа дисциплины «Права на результаты интеллектуальной деятельности».

– Рабочая программа дисциплины «Основы НТИ и информационная поддержка НИ».

– Рабочая программа дисциплины «Основы промышленной метрологии и калибровки».

– Рабочая программа педагогической практики.

2.2.4. Итоговая аттестация проводится на кафедре Информационной безопасности

2.3.Условия реализации основной образовательной программы подготовки аспирантов по научной специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность».

2.3.1. Материально-техническое обеспечение.

Университет обеспечивает аспиранту доступ к научно-исследовательской инфраструктуре в соответствии с программой аспирантуры и индивидуальным планом работы.

Структурные подразделения, обеспечивающие процесс подготовки по научной специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность» располагают материально-технической базой, обеспечивающей проведение всех видов теоретической и практической подготовки, предусмотренных учебным планом аспиранта, включает в себя лабораторное оборудование для проведения научных исследований, обеспечения учебных дисциплин и практик.

Конкретное материально-техническое обеспечение и права доступа аспиранта к информационным ресурсам определяется научным руководителем конкретного аспиранта, исходя из направления научных исследований, тем учебных дисциплин и задания на практику.

2.3.2. Учебно-методическое обеспечение

Данная программа аспирантуры обеспечена необходимой учебно-методической литературой в печатном и/или электронном виде по всем структурным элементам учебного плана. Обеспеченность учебными изданиями – не менее одного учебного издания в печатной и/или электронной форме, достаточного для освоения программы аспирантуры на каждого аспиранта по каждой дисциплине, входящей в учебный план.

Каждый обучающийся по программе аспирантуры в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронно-библиотечным системам (ЭБС) и к электронной информационно-образовательной среде (ЭИОС) Университета. ЭИОС обеспечивает аспиранту доступ ко всем электронным ресурсам, которые сопровождают научно-исследовательский и образовательный процессы подготовки научных и научно-педагогических кадров в аспирантуре, согласно программе аспирантуры, в том числе к информации об итогах промежуточной аттестации с результатами выполнения индивидуального плана работы. Доступ возможен из любой точки, в которой имеется доступ к сети Интернет.

Аспирантам обеспечен доступ к следующим профессиональным базам данных, информационным справочным и поисковым системам:

ЛАНЬ: электронно-библиотечная система. – URL: https://e.lanbook.com (дата обращения: 01.03.2022).

ФСТЭК России. – URL: https://fstec.ru/ (дата обращения: 01.03.2022).

eLIBRARY.RU: научная электронная библиотека. – URL: http://www.elibrary.ru (дата обращения: 01.03.2022).

Scopus: наукометрическая база данных. – URL: http://www.scopus.com (дата обращения: 01.03.2022).

Web of Science: наукометрическая база данных URL: http://apps.webofknowledge.com (дата обращения: 01.03.2022).

Использование информации, в том числе обмен информацией, осуществляется с соблюдением требований российского и международного законодательства.

2.3.3. Кадровое обеспечение

Реализация программы аспирантуры обеспечивается научными и научно-педагогическими работниками Университета, имеющими ученую степень или опыт деятельности в соответствующей профессиональной сфере и систематически занимающимися научно-исследовательской деятельностью. 60% численности штатных научных или научно-педагогических работников, участвующих в реализации программы аспирантуры по научной специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность» имеют ученую степень и/ или ученое звание.

Научные руководители, назначенные аспирантам, имеют ученую степень, осуществляют научную (научно-исследовательскую) деятельность по соответствующему направлению исследований в рамках научной специальности, имеют публикации по результатам указанной научно-исследовательской деятельности в рецензируемых отечественных и/или зарубежных научных журналах и изданиях. Научными руководителями осуществляется апробация результатов указанной научной (научно-исследовательской) деятельности на российских и/или международных конференциях, в том числе в течение трех последних лет.

ЛИСТ СОГЛАСОВАНИЯ

Программа аспирантуры по научной специальности по научной специальности – 2.3.6 «Методы и системы защиты информации, информационная безопасность» разработана на кафедре «Информационная безопасность».

Заведующий кафедрой «Информационная безопасность» _____ Хорев А.А.

Согласовано:

Проректор по НР _____ Дронов А.А.

Научный руководитель специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность»

_____ Хорев А.А.

Начальник ОДА _____ Романенко Ю.М.