М МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЧАСТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МЕЖДУНАРОДНАЯ АКАДЕМИЯ ВЫСОКИХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ОБРАЗОВАНИИ» (ЧОУ ВО «МАВИТО»)
ИНН 6732243429, КПП 673201001, 214000 г. Смоленск, ул. Ленина, 16, 2 этаж, ОГРН 1236700002220
Р/с 40703810659000000114, Смоленское отделение №8609 ПАО СБЕРБАНК, к/с 30101810000000000632,
БИК 046614632 https://мавито.рф E-mail mavito67@yandex.ru Тел.: 8800 707-1326, +79915206125

УТВЕРЖДАЮ:
Ректор ЧОУ ВО «МАВИТО»

_____ В.А. Благовестов
«10» января 2026 г.

Рассмотрено на заседании
Ученого совета ЧОУ ВО «МАВИТО»,
протокол № 1/01 от «10» января 2026 г.

О направлениях научной (научно-исследовательской) деятельности ЧОУ ВО «МАВИТО»

Приоритетные направления научной (научно-исследовательской) деятельности

Приоритетом научной (научно-исследовательской) деятельности ЧОУ ВО «МАВИТО» (далее -Академия) на период 2026 - 2029 гг. является направление «Информационная безопасность».

Информационная безопасность — научное направление, изучающее методы и средства защиты информации и информационных систем от несанкционированного доступа, использования, раскрытия, искажения, модификации или уничтожения. Ключевая цель направления — обеспечить три базовых свойства защищаемой информации: конфиденциальность (доступ только для уполномоченных субъектов); целостность (сохранение точности и полноты данных); доступность (возможность получить информацию в нужный момент). Направление охватывает разработку технических, организационных, правовых и иных механизмов защиты — с учётом актуальных угроз и рисков.

Научно-исследовательская база

Научно-исследовательская база Академии по направлению «Информационная безопасность» включает комплекс ресурсов, инфраструктуры, технологий и партнёрских связей, которые обеспечивают проведение исследований, разработку новых решений и подготовку квалифицированных специалистов.

Ключевыми компонентами научно-исследовательской базы являются:

- Лаборатории и специализированные помещения. Оснащены современным оборудованием, специализированными серверами, инструментами мониторинга для анализа киберугроз.
- Программное обеспечение и инструменты, включая средства для сканирования уязвимостей, инструменты для анализа журналов, песочницы для безопасного тестирования подозрительных файлов и приложений.
- Базы данных и библиотеки. Доступ к актуальным научным публикациям, отраслевым отчётам, базам знаний по кибербезопасности.
- Партнёрства с IT-компаниями и отраслевыми организациями. Сотрудничество с компаниями, разрабатывающими решения в сфере ИБ, доступ к передовым технологиям.
- Нормативно-правовая база и методические материалы. Сборники стандартов (ISO/IEC 27001, NIST, ФЗ «О персональных данных» и др.), шаблоны документации для сертификации систем защиты информации, методические рекомендации по проведению аудитов и оценок рисков.
- Системы для анализа инцидентов. Инструменты для расследования кибератак, которые позволяют изучать реальные кейсы и разрабатывать методы их предотвращения.
- Образовательные программы и курсы. Разработка специализированных учебных планов, включающих актуальные дисциплины по кибербезопасности, пентестингу, защите ИИ-систем, анализу угроз в IoT и других направлениях.
- Партнёрство с онлайн-платформами для дополнительного обучения, сотрудничество с регуляторами (ФСТЭК, ФСБ и др.) для работы над проектами, связанными с защитой критической информационной инфраструктуры.

При формировании научно-исследовательской базы применяется комплексный подход, включающий материально-техническое оснащение, развитие кадрового потенциала, установление партнёрских связей и постоянное обновление ресурсов в соответствии с быстроменяющимся ландшафтом угроз.

Результаты научной (научно-исследовательской) деятельности

Результатами научной (научно-исследовательской) деятельности Академии по направлению «Информационная безопасность» являются достижения, связанные с разработкой методов, технологий, методик, теоретических основ и практических решений в этой области.

Направления и формы результатов научной (научно-исследовательской) деятельности:

- Теоретические исследования и разработки:

  анализ и систематизация угроз информационной безопасности, включая их классификацию, динамику и влияние на образовательные процессы;

  исследование правовых и этических аспектов информационной безопасности, включая вопросы защиты персональных данных, интеллектуальной собственности и цифрового суверенитета;

  разработка теоретических основ для создания систем защиты информации в специфических средах (например, в системах электронного документооборота, образовательных платформах);

- Методологические разработки:

  создание методик оценки уровня защищённости информационных систем и образовательных ресурсов;

  разработка алгоритмов и методов обнаружения и предотвращения кибератак, анализа уязвимостей;

  создание методик обучения и повышения квалификации педагогов и студентов в области информационной безопасности;

  разработка подходов к интеграции вопросов информационной безопасности в учебные программы и образовательные стандарты.

- Технологические решения и разработки:

  применение технологий машинного обучения, нейросетей и других методов искусственного интеллекта для выявления инцидентов информационной безопасности.

- Экспериментальные и прикладные исследования:

  исследование уровня осведомлённости педагогов и студентов в вопросах информационной безопасности, анализ их потребностей и барьеров.

- Нормативно-методические разработки:

  создание внутренних нормативных документов, регламентов, инструкций для функционирования систем информационной безопасности в образовательных организациях.

- Образовательные продукты:

  разработка учебных курсов, онлайн-курсов, тренингов по информационной безопасности для разных категорий обучающихся (студенты, педагоги, работники, должностные обязанности которых связаны с обеспечением информационной безопасности);

  создание образовательных модулей, интерактивных ресурсов, лабораторных практикумов для изучения методов защиты информации.

- Публикационная активность.

- Социокультурные и просветительские проекты:

  программы по формированию информационной культуры и критического мышления у учащихся;

  мероприятия по повышению осведомлённости общественности о рисках и мерах защиты в информационном пространстве.

Результаты научной (научно-исследовательской) деятельности должны способствовать развитию научной базы в области информационной безопасности, практическому улучшению защищённости образовательных учреждений, подготовке квалифицированных специалистов, а также формированию культуры информационной безопасности среди участников образовательного процесса.