МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

**МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ГЕОДЕЗИИ И КАРТОГРАФИИ
(МИИГАиК)**

ПРИКАЗ

28.08.2026 **МОСКВА** № 483-01

Об утверждении и введении в действие
локальных нормативных актов МИИГАиК

В целях определения задач, принципов и порядка управления и обеспечение защиты информации в МИИГАиК, а также определения задач, функций, структуры Центра отраслевых мониторинговых систем и информационной безопасности (ЦОМСиИБ) Университета, руководствуясь Уставом МИИГАиК,

П Р И К А З Ы В А Ю:

1. Утвердить и ввести в действие с 28 августа 2026 г. Политику защиты информации в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии» (Приложение № 1 к настоящему приказу).
2. Утвердить и ввести в действие с 28 августа 2026 г. Положение о Центре отраслевых мониторинговых систем и информационной безопасности (ЦОМСиИБ) федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет геодезии и картографии» (Приложение № 2 к настоящему приказу).
3. Признать утратившим силу с 28 августа 2026 г. Положение о Центре отраслевых мониторинговых систем и информационной безопасности (ЦОМСиИБ) федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет геодезии и картографии», принятое решение ученого совета МИИГАиК 30 июня 2023 г. (протокол № 17), введенное в действие приказом ректора МИИГАиК от 30 июня 2023 г. № 319-01.
4. Административной службе Административно-правовой дирекции довести настоящий приказ до сведения соответствующих должностных лиц университета путем направления на адреса электронной почты.
5. Управлению информатизации Дирекции информационных технологий разместить настоящий приказ на официальном сайте МИИГАиК.
6. Контроль за исполнением настоящего приказа возложить на проректора Карпукова А.В.

Ректор **Н.Р. Камынина**

Проект приказа вносит:
Директор Центра отраслевых мониторинговых
система и информационной безопасности (ЦОМСиИБ)
С.С. Дубов

Согласовано:
проректор
А.В. Карпуков

Приложение № 2

к приказу ректора МИИГАиК

от 28 августа 2026 г. № 483-01

ПОЛОЖЕНИЕ

о Центре отраслевых мониторинговых систем и информационной безопасности (ЦОМСиИБ) федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет геодезии и картографии»

Москва, 2026

1. Общие положения

1.1. Настоящее Положение о Центре отраслевых мониторинговых систем и информационной безопасности (ЦОМСиИБ) федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет геодезии и картографии» (далее – Положение) является локальным нормативным актом федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет геодезии и картографии» (далее – Университет, МИИГАиК), определяющим цели деятельности, задачи, функции, структуру Центра отраслевых мониторинговых систем и информационной безопасности (ЦОМСиИБ) Университета (далее – подразделение, ЦОМСиИБ), права, обязанности, ответственность его работников и взаимодействие с другими структурными подразделениями Университета и сторонними организациями.

1.2. Настоящее Положение разработано в соответствии с:

— Федеральным законом от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;

— Трудовым кодексом Российской Федерации;

— Уставом Университета;

— Правилами внутреннего трудового распорядка Университета;

— иными локальными нормативными актами Университета.

1.3. Подразделение является структурным подразделением МИИГАиК, создается, реорганизуется и ликвидируется приказом ректора.

1.4. В своей деятельности подразделение руководствуется:

- Трудовым кодексом Российской Федерации;

- Федеральным законом от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;

— Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;

— Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»;

— Указом Президента РФ от 06.03.1997 №188 «Об утверждении Перечня сведений конфиденциального характера»;

— Постановлением Правительства Российской Федерации от 3 февраля 2012 г. №79 «О лицензировании деятельности по технической защите конфиденциальной информации»;

— Постановлением Правительства Российской Федерации от 16 апреля 2012 г. №313 «Об утверждении Положения о лицензировании деятельности по

разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)»;

— приказом ФСТЭК России от 18.02.2013 №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

— приказом ФСТЭК России от 11.04.2025 №117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений»;

— иными нормативно-правовыми актами Российской Федерации, регулирующими вопросы информационной безопасности и защиты информации;

— Уставом и иными локальными нормативными актами Университета;

— настоящим Положением.

2. Цели и задачи деятельности подразделения

2.1. Цели деятельности подразделения направлены на:

2.1.1. Развитие проектной деятельности Университета в сфере информационных технологий, территориального планирования, информационной безопасности и защиты информации.

2.1.2. Обеспечение необходимого уровня информационной безопасности в Университете в соответствии с законодательством Российской Федерации;

2.1.3. Обеспечение условий для проверки работ студентов и исследователей на наличие неправомочных заимствований.

2.2. Основными задачами деятельности подразделения являются:

2.2.1. Выполнение работ, оказание услуг в сфере информационных технологий, территориального планирования, информационной безопасности и защиты информации;

2.2.2. Разработка и реализация политики защиты информации МИИГАиК;

2.2.3. Выбор, внедрение и сопровождение системы проверки неправомочных заимствований;

3. Функции подразделения

3.1. Для выполнения работ, оказания услуг в сфере информационных технологий, территориального планирования, информационной безопасности и защите информации подразделение осуществляет следующие функции:

3.1.1. Организация и проведение встреч с потенциальными заказчиками работ, услуг в сфере информационных технологий, территориального планирования, информационной безопасности и защиты информации;

3.1.2. Анализ ресурсоемкости работ, услуг в сфере информационных технологий, территориального планирования, информационной безопасности и защиты информации;

3.1.3. Выполнение работ, оказание услуг в сфере информационных технологий, территориального планирования, информационной безопасности и защиты информации.

3.2. Для выполнения задачи по разработке и реализации политики защиты информации МИИГАиК подразделение осуществляет следующие функции:

3.2.1. Разработка и согласование локальных нормативных и распорядительных актов в области обеспечения информационной безопасности и защиты информации;

3.2.2. Контроль соблюдения требований законодательства и локальных нормативных актов в области обеспечения информационной безопасности и защиты информации;

3.2.3. Отслеживание изменений законодательства Российской Федерации в области обеспечения информационной безопасности и защиты информации;

3.2.4. Принятие мер по обеспечению функционирования применяемых средств криптографической защиты информации (далее – СКЗИ) в соответствии с условиями выданных на них сертификатов, а также контроль выполнения требований по установленному порядку учета и выдачи СКЗИ, носителей с ключевой информацией;

3.2.5. Организация обучения лиц, использующих СКЗИ, правилам работы с ними;

3.2.6. Принятие мер по предупреждению разглашения защищаемых сведений конфиденциального характера, а также возможной утечки таких сведений при выявлении фактов утраты или недостачи СКЗИ, ключевых документов к ним;

3.2.7. Организация подключения и сопровождение защищенных каналов связи;

3.2.8. Организация получения и настройка электронных подписей;

3.2.9. Формирование и реализация политики прав доступа к информационным системам и сервисам МИИГАиК;

3.2.10. Осуществление мероприятий по подключению МИИГАиК к внешним информационным системам и сервисам;

3.2.11. Закупка, установка, монтаж и наладка средств защиты;

3.2.12. Подача уведомлений, предусмотренных законодательством Российской Федерации в области персональных данных, в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций;

3.2.13. Организация работ по выявлению оценке уязвимостей и актуальных угроз безопасности информации в Университете;

3.2.14. Разработка, внедрение и контроль соблюдения конфигураций для используемых информационных систем, сетевого оборудования и средств вычислительной техники;

3.2.15. Управление процессами своевременного обновления системного и прикладного программного обеспечения;

3.2.16. Организация защиты и контроля информации при обработке, хранении и обращении с информацией ограниченного доступа в Университете;

3.2.17. Обеспечение безопасности информации при применении конечных устройств;

3.2.18. Обеспечение защиты информации при применении мобильных устройств;

3.2.19. Обеспечение защиты информации при удаленном доступе пользователей к информационным системам;

3.2.20. Обеспечение защиты информации при беспроводном доступе пользователей к информационным системам;

3.2.21. Обеспечение защиты информации при предоставлении пользователям доступа к информационным системам, предусматривающего чтение, выполнение, изменение, запись, удаление программ и (или) данных в информационных системах;

3.2.22. Обеспечение мониторинга информационной безопасности;

3.2.23. Обеспечение разработки безопасного программного обеспечения;

3.2.24. Обеспечение непрерывности функционирования информационных систем при возникновении нештатных ситуаций;

3.2.25. Разработка обязательных для исполнения требований по информационной безопасности при заключении договоров (соглашений) со сторонними организациями;

3.2.26. Обеспечение защиты от компьютерных атак, направленных на отказ в обслуживании;

3.2.27. Реализация в информационных системах мер по их защите и защите, содержащейся в них информации;

3.2.28. Обеспечение непрерывного взаимодействия с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

3.2.29. Формирование и направление отчетной документации по результатам мониторинга информационной безопасности, сбор исходных данных и расчет показателей защищенности (далее - Кзи) и уровня зрелости (далее - Пзи) системы защиты информации руководству Университета и во ФСТЭК России в соответствии с установленными нормативными требованиями;

3.2.30. Организация и проведение регулярного контроля уровня защищенности информации в информационных системах Университета;

3.2.31. Организация обучения, повышения уровня знаний и информированности работников Университета по вопросам соблюдения требований информационной безопасности;

3.2.32. Определение, систематизация и актуализация перечня событий безопасности в информационных системах Университета, наступление которых может повлечь за собой нарушение целей защиты информации;

3.2.33. Планирование состава, периодичности и сроков проведения мероприятий по обеспечению защиты информации, а также проведение ресурсного анализа и обоснования для реализации защитных мер;

3.2.34. Выполнение иных функций, исходя из поставленных руководством целей и задач в рамках обеспечения информационной безопасности в Университете.

3.3. Для выполнения задачи по выбору, внедрению и сопровождению системы проверки неправомочных заимствований подразделение осуществляет следующие функции:

3.3.1. Определение технических требований, обеспечение приобретения, организация подключения и администрирование системы проверки неправомочных заимствований.

3.4. Типовые функции Подразделения:

3.4.1. подготовка проектов локальных нормативных актов в части, касающейся деятельности Подразделения, их актуализация и согласование с проректорами по направлениям деятельности;

3.4.2. подготовка проектов ответов на запросы органов власти, местного самоуправления, обращения (заявления, жалобы, претензии и т.п.) организаций и физических лиц, касающиеся деятельности Подразделения;

3.4.3. сбор, обработка и анализ данных по показателям, формирование отчетов, и их направление (размещение в информационных системах) в Минобрнауки России, органы статистики, федерального казначейства, налоговые органы и т.п., в части, касающейся деятельности Подразделения;

3.4.4. ведение делопроизводства и формирование номенклатуры дел Подразделения в соответствии с локальными нормативными актами МИИГАиК, Федеральным законом от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации», Приказом Росархива от 20.12.2019 № 236, Приказом Росархива от 31.07.2023 № 77 и ГОСТ Р 7.0.97-2025 «Система стандартов по информации, библиотечному и издательскому делу. Организационно-распорядительная документация. Требования к оформлению документов», приказом Минобрнауки России от 29.11.2023 № 1111;

3.4.5. обработка персональных данных в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ и локальными нормативными актами Университета;

3.4.6. организация защиты конфиденциальной информации;

3.4.7. участие в реализации антикоррупционной политики Университета;

3.4.8. организация соблюдения требований безопасности, охраны труда и пожарной безопасности;

3.4.9. планирование потребности Подразделения в работниках, обучении и повышении квалификации работников;

3.4.10. планирование потребности Подразделения в помещениях, оборудовании, оргтехнике, инструментах, расходных материалах, программном обеспечении, доступа к IT-инфраструктуре, профессиональным ресурсам, информационным и специализированным системам, предложения по включению в план ФХД;

3.4.11. контроль состояния и рационального использования помещений, оборудования, оргтехники, инструментов, материалов, экономное их использование;

3.4.12. подготовка документации для приобретения товаров, оказания услуг, выполнения работ для нужд МИИГАиК, включая формирование заявок на закупку, разработку технической документации (технического задания), обоснование заключения договора/контракта с единственным поставщиком;

3.4.13. сопровождение исполнения договора/контракта, контроль за фактическим исполнением, соблюдением промежуточных сроков, сроков окончания договора/контракта, обоснование заключения дополнительного соглашения для нужд МИИГАиК;

3.4.14. осуществление приемки товаров, работ, услуг (при необходимости организация комиссионной приемки) по договорам/контрактам, контроль за своевременностью предоставления документов на оплату (счетов, счетов-фактур, товарных накладных, актов приемки и других первичных документов, подписанных и оформленных в соответствии с предъявляемыми к таким документам требованиями);

3.4.15. обеспечение рационального использования работниками Подразделения товаров, результатов работ, контроль за течением сроков годности, в пределах которых могут быть предъявлены требования в отношении недостатков товаров и результатов работ;

3.4.16. своевременное обеспечение Пресс-службы МИИГАиК и Управления информатизации Университета актуальной информацией, касающейся деятельности Подразделения, для её размещения на официальном сайте Университета и (или) на официальных страницах Университета в социальных сетях в информационно-телекоммуникационной сети «Интернет».

4. Структура

4.1. Координацию деятельности подразделения осуществляет проректор Университета, курирующий вопросы по защите информации (далее – курирующий проректор).

4.2. Структура и штатная численность подразделения определяются приказом ректора Университета.

4.3. Подразделение возглавляет директор, назначаемый на должность и освобождаемый от должности приказом ректора Университета, который осуществляет непосредственное руководство подразделением и подчиняется курирующему проректору Университета.

4.4. Работа подразделения организуется в соответствии с настоящим Положением, Уставом Университета, решениями Ученого совета Университета, приказами и распоряжениями ректора Университета, поручениями курирующего проректора Университета.

4.5. Работники подразделения выполняют свои должностные обязанности в соответствии с трудовым договором, заключаемым с каждым работником, настоящим Положением и должностными инструкциями, утвержденными ректором Университета.

4.6. Работники подразделения докладывают директору о выполнении соответствующих поручений.

5. Права, обязанности и ответственность работников подразделения

5.1. При выполнении своих должностных обязанностей работники подразделения имеют право:

5.1.1. запрашивать через директора и получать от руководителей структурных подразделений Университета информацию, документы и материалы, необходимые для решения вопросов, связанных с выполнением возложенных на подразделение задач и функций;

5.1.2. представлять Университет в органах государственной власти и местного самоуправления, иных органах, учреждениях и организациях по вопросам, входящим в компетенцию подразделения, на основании доверенности, выданной ректором Университета;

5.1.3. давать разъяснения и рекомендации по вопросам, входящим в компетенцию подразделения;

5.1.4. участвовать в конференциях, совещаниях, семинарах разного уровня по вопросам, входящим в компетенцию подразделения;

5.1.5. знакомиться с документами, касающимися деятельности подразделения;

5.1.6. сообщать обо всех выявленных в процессе своей деятельности нарушениях и вносить предложения по их устранению;

5.1.7. вносить предложения по совершенствованию работы подразделения.

5.2. Работники подразделения обязаны:

5.2.1. соблюдать законодательство Российской Федерации, Устав Университета, Правила внутреннего трудового распорядка, настоящее Положение и иные локальные нормативные акты Университета, касающиеся деятельности подразделения;

5.2.2. своевременно, качественно и в полном объеме выполнять должностные обязанности.

5.3. Всю полноту ответственности за качество и своевременность выполнения задач и функций подразделения несет директор.

5.4. Персональная ответственность работников подразделения устанавливается в соответствии с их должностными инструкциями, трудовыми договорами.

6. Взаимодействие

6.1. Взаимодействие подразделения с другими структурными подразделениями Университета и сторонними организациями определяется задачами и функциями, возложенными на него настоящим Положением.

7. Заключительные положения

7.1. Настоящее Положение утверждается и вводится в действие приказом ректора Университета.