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 №1
к приказу ректора МИИГАиК
от 28 августа 2026 г. № 483-01

П О Л И Т И К А

защиты информации в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии»

Москва, 2026

1. Общие положения

1.1. Настоящая Политика защиты информации в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии» (далее - Политика) является локальным нормативным актом федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет геодезии и картографии» (далее – Оператор, Университет) и определяет цели, задачи, принципы, основные объекты и угрозы объектам защиты, порядок управления и обеспечение защиты информации в Университете.

1.2. Настоящая Политика направлена на защиту объектов, информационной инфраструктуры и процессов обработки информации Университета от возможного нанесения им материального, физического или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи ее по каналам связи, а также минимизацию подобных рисков.

1.3. Настоящая Политика распространяется:

- на все виды деятельности Университета;
- на всю обрабатываемую в Университете информацию;
- на любые информационные системы и ресурсы, средства обработки информации;
- на все формы представления информации – электронную, на бумажных носителях, устную (речевую), визуальную и иные формы;
- на все процессы обработки информации в Университете, включая, но не ограничиваясь деятельностью в области обработки и обеспечения безопасности персональных данных, защиты конфиденциальной информации, в том числе составляющей коммерческую тайну, сведений, связанных с профессиональной деятельностью;
- на всех работников и обучающихся Университета, а также третьих лиц, с которыми Университетом заключены договоры гражданско-правового характера с условием соблюдения ими настоящей Политики.

1.4. Настоящая Политика разработана в соответствии с:

— 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 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

— 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»;

— Методическим документом ФСТЭК России от 12.04.2026 «Состав и содержание мероприятий и мер по защите информации, содержащейся в информационных системах»;

— национальными стандартами Российской Федерации в области защиты информации и информационной безопасности;

— иными нормативными правовыми актами Российской Федерации, регулирующими вопросы защиты информации;

— Уставом и иными локальными нормативными актами Университета.

1.5. Для целей настоящей Политики используются следующие понятия:

— информация - сведения (сообщения, данные) независимо от формы их представления;

— защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации;

— объект защиты - это информация или ресурс информационной системы, имеющие ценность для Университета, использующиеся для достижения целей Университета,

— персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных);

— безопасность информации (данных) – состояние защищенности информации (данных), при которой обеспечиваются ее (их) конфиденциальность, доступность и целостность;

— событие безопасности - события, связанные с возможным нарушением безопасности информации, нарушением функционирования информационных систем, реализацией угроз безопасности информации;

— инцидент безопасности - это событие (или группа событий), которые могут привести или уже привели к успешной кибератаке, нарушению работы объекта защиты, нанесению ущерба интересам Оператора;

— уязвимость – слабость в средствах защиты, которую можно использовать для нарушения информационной системы или содержащейся в ней информации;

— средство защиты информации - техническое, программное или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа к информации или ресурсам информационной системы;

— средство криптографической защиты информации – технические, криптографические, программные и другие средства, предназначенные для защиты охраняемой информации, в которых для обеспечения безопасности охраняемой информации осуществляется ее криптографическое преобразование.

2. Цели и задачи защиты информации

2.1. Университет обеспечивает защиту информации в целях:

— недопущения (снижения возможности) наступления негативных последствий (событий) от нарушения конфиденциальности, целостности, доступности информации;

— недопущения (снижения возможности) наступления негативных последствий (событий) от нарушения функционирования информационных систем вследствие реализации (возникновения) угроз безопасности информации.

2.2. Для достижения целей Университет обеспечивает выполнение следующих задач:

— определение недопустимых событий, связанных с нарушением безопасности информации;

— систематическое выявление и оценка угроз безопасности информации;

— реализация организационных и технических мер защиты информации, адекватных актуальным угрозам и классу защищённости информационных систем;

— управление конфигурациями информационных систем и их уязвимостями;

— непрерывный мониторинг информационной безопасности и реагирование на инциденты;

— обеспечение физической защиты компонентов информационных систем;

— поддержание необходимого уровня знаний пользователей по вопросам защиты информации.

3. Принципы защиты информации

3.1. В основе реализации обеспечения защиты информации лежит комплексный подход, который включает в себя следующие группы мер защиты информации:

— правовые;

— организационные;

— программно-технические.

3.2. Деятельность по защите информации в Университете основывается на следующих ключевых принципах:

— законность;

— признание, соблюдение и защита прав и свобод человека и гражданина;

— сотрудничество и взаимопонимание;

— персональная ответственность и осведомленность;

— экономическая целесообразность;

— комплексность применения правовых, организационных и технических мер;

— неотъемлемость защиты информации;

— системность и своевременность регламентации процессов защиты информации;

— непрерывность защиты информации;

— гибкость и управляемость применения системы защиты информации.

4. Основные объекты защиты

4.1. Основными объектами защиты Оператора являются:

— информация, составляющая персональные данные, секрет производства (ноу-хау), коммерческую тайну, служебную информацию, внутренние документы Оператора, иная информация, чувствительная по отношению к случайным и несанкционированным воздействиям и нарушению их безопасности (в том числе открытая (общедоступная)

информация), представленная в виде документов и информационных массивов, независимо от формы и вида их представления;

— информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства обработки, передачи и отображения информации, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены чувствительные компоненты информационной системы;

— процессы обработки информации в информационной системе - информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, процессы жизненного цикла информационной системы.

5. Основные угрозы объектам защиты

5.1. Основные угрозы объектам защиты Оператора подразделяются на следующие группы:

— угрозы конфиденциальности, а именно несанкционированный доступ, разглашение защищаемой информации, а также компрометация учетных данных (паролей, идентификаторов) и ключей доступа;

— угрозы целостности, а именно несанкционированное или некорректное изменение данных и настроек информационных систем, нештатные режимы работы программного обеспечения, а также вирусные заражения и осуществление несанкционированных сетевых атак;

— угрозы доступности, а именно уничтожение или утеря информации, выход из строя программно-технических средств, материальных носителей и нарушение функционирования технических мер защиты.

6. Меры защиты в информационных системах

6.1. Для достижения поставленных целей и задач применяются следующие меры:

— идентификация и аутентификация субъектов доступа;

— управление доступом;

— защита машинных носителей информации;

— регистрация событий безопасности;

— антивирусная защита;

— контроль целостности;

— защита информации при удалённом доступе;

— обеспечение непрерывности функционирования информационных систем при нештатных ситуациях.

7. Система управления деятельностью по защите информации. Категории лиц, участвующих в защите информации, их обязанности и полномочия.

7.1. Управление защитой информации обеспечивается как при осуществлении информационного обмена внутри Университета, так и при взаимодействии со сторонними организациями и третьими лицами.

7.2. В систему управления деятельностью по защите информации в Университете входят:

— ректор Университета;

— проректор, курирующий инфраструктурное развитие и безопасность;

— Центр отраслевых мониторинговых систем и информационной безопасности (далее – ЦОМСиИБ).

7.3. Категории лиц, участвующих в защите информации, их обязанности и полномочия:

7.3.1. ректор Университета утверждает локальные нормативные акты, назначает ответственных лиц в области защиты информации, издает распоряжения о проведении служебных проверок по фактам выявленных нарушений в области защиты информации;

7.3.2. проректор, курирующий инфраструктурное развитие и безопасность, осуществляет ресурсное обеспечение мероприятий по защите информации, инициирует служебные проверки, дает обязательные для исполнения указания в пределах своей компетенции и инициирует служебные проверки по фактам выявленных нарушений;

7.3.3. руководитель Центра отраслевых мониторинговых систем и информационной безопасности контролирует соблюдение нормативно-правовых актов, локальных нормативных актов Университета, регулирующих вопросы защиты информации, и выполнение организационных и технических мер защиты, координирует деятельность работников по защите информации, обеспечивает реализацию организационных и технических мер защиты, контролирует законность обработки персональных данных в Университете. Руководитель Центра отраслевых мониторинговых систем и информационной безопасности вправе требовать от структурных подразделений и работников Университета соблюдения правил обработки персональных данных, приостанавливать эксплуатацию оборудования при выявлении угроз безопасности и инициировать служебные проверки по фактам выявленных нарушений;

7.3.4. работники Центра отраслевых мониторинговых систем и информационной безопасности участвуют в разработке и актуализации локальных нормативных актов, регулирующих вопросы защиты информации, и процессе реализации организационных и технических мер защиты информации, выявляют инциденты и принимают меры по реагированию на них, настраивают и эксплуатируют средства защиты информации, средства криптографической защиты информации, а также выполняют иные распоряжения курирующего проректора, непосредственного руководителя, вносят предложения по оптимизации процессов защиты информации в Университете, запрашивают у структурных подразделений Университета, обеспечивающих техническое обслуживание, информацию, необходимую для выполнения обязанностей по защите информации;

7.3.5. работники Дирекции информационных технологий осуществляют обновление и техническое обслуживание серверной и сетевой инфраструктуры, обеспечивают бесперебойную работу технических средств, оформляют в установленном порядке изменения в части информационных технологий инфраструктуры Университета и своевременно уведомляют о них руководителя Центра отраслевых мониторинговых систем и информационной безопасности (лица, его замещающего), сообщают о выявленных нарушениях, инцидентах и подозрительной активности в работе информационных систем, вносят предложения о закупке оборудования в рамках утвержденных процедур, а также о выводе из эксплуатации подлежащих замене программных и технических средств;

7.3.6. внутренние и внешние пользователи информационных систем, получившие доступ к информационным системам, ресурсам и данным в объеме, необходимом для

выполнения должностных обязанностей либо для освоения образовательной программы, либо для исполнения гражданско-правового договора, заключенного с МИИГАиК, используют предоставленные программные и технические средства в соответствии с их назначением, сообщают в техническую поддержку данной информационной системы об инцидентах и подозрительной активности в работе информационных систем.

7.4. Защите подлежит любая информация, принадлежащая Оператору или переданная Оператору контрагентом на основании заключенного с МИИГАиК гражданско-правового договора. Для всех объектов защиты Оператора устанавливаются меры безопасности в соответствии с их степенью важности для достижения целей Оператора.

7.5. Обязательства третьих лиц, которым предоставляется доступ с иным объемом прав к информационным системам Оператора, определяются условиями заключаемых с такими лицами договоров.

8. Ответственность

8.1. Соблюдение требований и правил в области защиты информации является обязательным для всех работников и обучающихся в Университете, а также третьих лиц, с которыми Университетом заключены договоры гражданско-правового характера с условием соблюдения ими настоящей Политики.

8.2. Лица, виновные в нарушении требований защиты информации, несут дисциплинарную, гражданско-правовую, административную и уголовную ответственность в соответствии с законодательством Российской Федерации.

9. Заключительные положения

9.1. Настоящая Политика вступает в силу с момента ее утверждения приказом ректора Университета.

9.2. Настоящая Политика подлежит пересмотру в случаях:

— изменения законодательства РФ, нормативных документов ФСТЭК России, ФСБ России и других документов в области защиты информации;

— изменений в информационной инфраструктуре или организационной структуре Университета.