МИНПРОСВЕЩЕНИЯ РОССИИ

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Нижегородский государственный педагогический
университет имени Козьмы Минина»
(Мининский университет)

ПРИКАЗ

25.03.2026 № 348/ОД

г. Нижний Новгород

Об утверждении Политики
информационной безопасности

В целях обеспечения выполнения требований законодательства Российской Федерации в области защиты информации и персональных данных, в том числе Федерального закона от 27.07.2006 года №152-ФЗ «О персональных данных» и Федерального закона от 27.07.2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации», а также организации защиты информационных ресурсов Мининского университета от несанкционированного доступа п р и к а з ы в а ю:

1. Утвердить:

1.1. Политику информационной безопасности Мининского университета (далее — Политика) согласно Приложению к настоящему приказу.

2. Установить:

2.1. Политика является обязательной для исполнения:

- всеми работниками Университета,
- структурными подразделениями,
- лицами, имеющими доступ к информационным ресурсам.

2.2. Требования Политики распространяются на:

- информационные системы,
- базы данных,
- рабочие станции,
- серверное и сетевое оборудование,
- учетные записи пользователей,
- официальный сайт и иные цифровые ресурсы.

3. Возложить:

3.1. Координацию технической реализации требований Политики в части эксплуатации информационных систем и средств защиты информации на начальника управления информационных технологий.

3.2. Осуществление организации выполнения мероприятий технического характера и контроль их исполнения в пределах своей компетенции на начальника УИТ:

- организация защиты информации,
- контроль управления доступом,
- учет пользователей,
- контроль резервного копирования,

- применение средств защиты,
- контроль обновлений ПО,
- участие в расследовании инцидентов,
- проведение внутренних проверок.

4. Руководителям структурных подразделений:
   - обеспечивать соблюдение требований Политики,
   - инициировать предоставление/изменение/блокировку доступа,
   - не допускать размещения ПДн и конфиденциальной информации без оснований,
   - обеспечивать актуальность размещаемой информации,
   - незамедлительно сообщать об инцидентах ИБ.
5. Установить:
   - доступ предоставляется только по служебной необходимости,
   - доступ осуществляется по индивидуальным учетным записям,
   - учетные записи уволенных сотрудников блокируются незамедлительно,
   - действия пользователей могут подлежать контролю.
6. Назначить ответственным за функционирование информационных систем и официального сайта начальника УИТ Сальникова Д.К.
7. Руководителям структурных подразделений обеспечить доведение настоящего приказа и Политики до сведения работников.
8. Директору центра стратегических коммуникаций и информационной политики Князевой О.В. обеспечить размещение приказа и Политики на официальном сайте Университета.
9. Контроль исполнения настоящего приказа возложить на проректора по цифровой трансформации Маркова К.А.

Ректор  В.В. Сдобняков

Приложение к приказу
ФГБОУ ВО «НГПУ им. К. Минина»
от «25» марта 2026г. № 348/ОД

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. **Общие положения**

1.1. Настоящая Политика устанавливает обязательные требования к обеспечению информационной безопасности.

1.2. Политика разработана в соответствии с:

- Федеральным законом от 27.07.2006 года №152-ФЗ «О персональных данных»,
- Федеральным законом от 27.07.2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации».

1.3. Цель — предотвращение:

- несанкционированного доступа,
- утечки информации,
- нарушения целостности,
- нарушения доступности.

2. **Объекты защиты**

- информационные системы,
- базы данных,
- персональные данные,
- серверы и АРМ,
- учетные записи,
- сетевая инфраструктура,
- резервные копии.

3. **Роли и ответственность**

3.1 Руководители структурных подразделений:

- обеспечивают организационные условия для выполнения требований политики информационной безопасности,
- определяют необходимость и уровень доступа к объектам защиты,

- контролируют сотрудников.

3.2 Ответственный за организацию обработки персональных данных (ПДн) отвечает за правовые основания обработки, состав персональных данных и соблюдение требований законодательства Российской Федерации.

3.3 Ответственный за информационную безопасность (ИБ) осуществляет:

- контроль ИБ,
- управление доступом к объектам защиты,
- аудит объектов защиты,
- реагирование на инциденты.

3.4 Пользователи обязаны:

- не передавать учетные данные посторонним лицам,
- использовать системы только по назначению,
- сообщать об инцидентах.

4. **Управление доступом к объектам защиты**

- доступ к объектам защиты осуществляется только по необходимости,
- использование индивидуальных учетных записей,
- запрет общих аккаунтов,
- регулярный пересмотр прав доступа,
- немедленная блокировка доступа к объектам защиты при увольнении сотрудника.

5. **Обеспечение безопасности учетных записей**

- уникальные логины,
- контроль прав,
- блокировка неиспользуемых учетных записей,
- запрет передачи своих учетных данных посторонним лицам.

6. **Автоматизированные рабочие места** (АРМ)

АРМ являются служебными ресурсами.

6.1 Установить, что вся информация на рабочих компьютерах является служебной информацией Университета.

6.2 Запрещается:

- хранить личные файлы (фото, видео, документы) на рабочем АРМ,
- использовать АРМ в личных целях,
- заходить в личные социальные сети без служебной необходимости,
- использовать личное облачное хранилище с рабочего компьютера,
- устанавливать программное обеспечение без разрешения.

6.3 Установить, что

- данные на АРМ подлежат контролю ответственных за организацию обработки персональных данных и администратора безопасности,
- АРМ могут проверяться ответственными за организацию обработки персональных данных и администратором безопасности,
- личные данные не защищаются.

7. **Антивирусная защита**

- обязательна на всех устройствах,
- подлежит регулярному обновлению,
- не может быть отключена.

8. **Сетевая безопасность обеспечивается следующим:**

- ограничение доступа,
- защита оборудования,
- контроль подключений,
- запрет использования несанкционированных устройств.

9. **Резервное копирование** – важный элемент обеспечения ИБ, предполагающий:

- обязательное резервное копирование,
- хранение резервных копий отдельно,
- контроль восстановления данных.

10. **Инциденты ИБ**

К инцидентам относятся:

- утечка,

- вирусы,
- взлом,
- потеря данных.

План действий при инциденте:

- фиксация,
- устранение,
- анализ.

11. **Контроль и аудит**
    - проверка соблюдения требований Политики информационной безопасности не реже 1 раза в год,
    - контроль доступа,
    - контроль резервного копирования,
    - контроль использования антивируса.
12. **Ответственность за нарушение требований Политики**
    - дисциплинарная ответственность,
    - ответственность в соответствии с законодательством РФ.