



**Администрация
Тонкинского муниципального округа
Нижегородской области
Распоряжение**

14.08.2026

№ 89-р

**Об утверждении Политики парольной защиты для
автоматизированных рабочих мест администрации Тонкинского
муниципального округа Нижегородской области и ее структурных
подразделений, наделенных правами юридического лица**

В соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»:

1. Утвердить прилагаемую Политику парольной защиты для автоматизированных рабочих мест администрации Тонкинского муниципального округа Нижегородской области и ее структурных подразделений, наделенных правами юридического лица (далее - Политика).

2. Руководителям структурных подразделений администрации Тонкинского муниципального округа Нижегородской области, в том числе наделенных правами юридического лица, обеспечить ознакомление сотрудников с Политикой под роспись.

3. Обнародовать настоящее распоряжение в порядке, установленном Уставом Тонкинского муниципального округа Нижегородской области, и разместить на официальном сайте Тонкинского муниципального округа Нижегородской области в информационно-телекоммуникационной сети «Интернет» по адресу: <https://tonkino.nobl.ru/>.

4. Настоящее распоряжение вступает в силу со дня его подписания.

5. Контроль за исполнением настоящего распоряжения возложить на заместителя главы администрации Тонкинского муниципального округа Нижегородской области Кононова Е.В.

Глава местного самоуправления



Ю.А.Смирнов

УТВЕРЖДЕНА
распоряжением администрации
Тонкинского муниципального округа
Нижегородской области
от 14.08.2026 № 89-р

ПОЛИТИКА
парольной защиты для автоматизированных рабочих мест администрации
Тонкинского муниципального округа Нижегородской области и ее
структурных подразделений, наделенных правами юридического лица

1. Общие положения

1.1. Настоящая Политика определяет обязательные требования к минимальным характеристикам и защите паролей учетных записей пользователей, администраторов и сервисных служб на автоматизированных рабочих местах (далее - АРМ) в администрации Тонкинского муниципального округа Нижегородской области и ее структурных подразделениях, наделенных правами юридического лица (далее - Администрация).

1.2. Политика устанавливает единые требования к созданию, использованию, хранению, смене и прекращению действия паролей локальных и доменных учетных записей АРМ.

1.3. Положения настоящей Политики применяются ко всем АРМ, вводимым в эксплуатацию и эксплуатируемым в составе информационной инфраструктуры Администрации, включая мобильные устройства доступа.

1.4. Требования Политики распространяются как на стандартные пользовательские учетные записи, так и на привилегированные (администраторы локальных машин, системные администраторы).

1.5. Политика не применяется к системам, предназначенным для обработки информации, составляющей государственную тайну.

2. Требования к паролям

2.1. Длина пароля.

Минимальная длина пароля должна составлять двенадцать (12) символов. Для сервисных учетных записей рекомендуется использование длинных парольных фраз от 20 символов.

2.2. Сложность пароля.

Пароль должен состоять из символов не менее чем трех различных групп:

а) прописные буквы латинского алфавита (A-Z);

- б) строчные буквы латинского алфавита (a-z);
- в) арабские цифры (0-9);
- г) специальные символы (пример: ! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { | } ~).

Исключение: для стандартных пользовательских АРМ допускается снижение сложности до двух групп при условии использования многофакторной аутентификации.

2.3. Запрещенные к использованию данные.

Запрещается формирование пароля на основе:

- а) личной информации пользователя (Ф.И.О. в любых комбинациях, дата рождения, номера документов, телефонов);
- б) инвентаризационных данных оборудования (инвентарный номер АРМ, серийный номер монитора или системного блока, сетевое имя компьютера);
- в) наименований структурных подразделений, должностей и общеизвестных фактов о деятельности Администрации;
- г) лексических единиц любого языка в неизменном виде («password», «admin», «qwerty», «user»);
- д) простых последовательностей символов («1234567890», «abcdef», повторяющихся блоков типа «PassPass»).

3. Требования к управлению жизненным циклом пароля

3.1. Срок действия пароля.

Максимальный срок действия пароля для учетных записей пользователей АРМ не должен превышать девяносто (90) календарных дней. Для учетных записей администраторов и привилегированных пользователей срок действия не должен превышать тридцати (30) календарных дней. Для сервисных учетных записей смена производится по факту компрометации или плановой ротации ключей.

3.2. Проверка на схожесть с предыдущими паролями.

Запрещается установка пароля, который является предсказуемой модификацией предыдущего (например, инкрементация цифр в конце, изменение регистра первой буквы, добавление одного спецсимвола).

4. Технические и организационные меры защиты

4.1. Защита от неавторизованного подбора.

Для всех типов учетных записей АРМ должна быть активирована функция автоматической блокировки сеанса доступа после превышения лимита неудачных попыток аутентификации.

4.2. Автоматическая блокировка экрана.

При простое АРМ без активности пользователя более 10 минут должно происходить автоматическое завершение сеанса или блокировка экрана,

требующая повторной аутентификации.

4.3. Многофакторная аутентификация (MFA).

Для удаленного доступа к ресурсам сети Администрации, а также для входа в систему под привилегированными учетными записями обязательно применение второго фактора подтверждения (ОТР-токены, аппаратные ключи, push-уведомления).

4.4. Передача и хранение вне системы.

Категорически запрещается записывать пароли на бумажных носителях, оставлять их на стикерах у рабочего места, сохранять в общедоступных текстовых файлах или передавать через открытые каналы связи (электронная почта, мессенджеры).

4.5. Ответственность.

Пользователь несет персональную ответственность за сохранность своего пароля. Передача учетных данных третьим лицам запрещена. О любом факте компрометации пароль должен быть немедленно изменен, а инцидент зарегистрирован.
