



**АДМИНИСТРАЦИЯ ПИЛЬНИНСКОГО МУНИЦИПАЛЬНОГО ОКРУГА
НИЖЕГОРОДСКОЙ ОБЛАСТИ
РАСПОРЯЖЕНИЕ**

от «19» августа 2026 года

№ 162

Об утверждении Политики парольной защиты автоматизированных рабочих мест (за исключением систем обработки сведений, составляющих государственную тайну)

В целях обеспечения безопасности процессов обработки информации ограниченного доступа, не отнесенной к государственной тайне, в администрации Пильнинского муниципального округа Нижегородской области и её структурных подразделениях, 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 Пильнинского муниципального округа Нижегородской области и её структурных подразделений (далее - Политика).
2. Руководителям структурных подразделений администрации Пильнинского муниципального округа Нижегородской области, обеспечить ознакомление сотрудников с Политикой под роспись.
3. Обнародовать настоящее распоряжение в порядке, установленном Уставом Пильнинского муниципального округа Нижегородской области, и разместить на официальном сайте Пильнинского муниципального округа Нижегородской области в информационно-телекоммуникационной сети «Интернет» по адресу: <https://pilna.nobl.ru/>.
4. Настоящее распоряжение вступает в силу со дня его подписания.
5. Контроль за исполнением настоящего распоряжения оставляю за главой местного самоуправления.

Глава местного самоуправления

Цапин Д.Н.

ПОЛИТИКА парольной защиты автоматизированных рабочих мест (за исключением систем обработки сведений, составляющих государственную тайну)

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 Пильнинского муниципального округа Нижегородской области и ее структурных подразделениях (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 базового уровня — не менее **8 символов**, для усиленного уровня (например, в финансовых организациях) рекомендуется уже **не менее 12 символов**. Для сервисных учетных записей рекомендуется использование длинных парольных фраз от **15 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 «PasswordPassword»).

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. Для всех типов учетных записей должна быть активирована функция автоматической блокировки (приостановки) сеанса доступа после превышения лимита неудачных попыток аутентификации. Рекомендуемые параметры: блокировка учетной записи на 30 минут после 5 неудачных попыток аутентификации в течение 5 минут.

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.