КОНТРОЛЬНО-СЧЕТНАЯ КОМИССИЯ ТОНКИНСКОГО МУНИЦИПАЛЬНОГО ОКРУГА НИЖЕГОРОДСКОЙ ОБЛАСТИ

ул. Ленина д.1, р.п. Тонкино, Нижегородская область, 606970
тел. (83153) 48-0-97, e-mail: ksk-tonkino@yandex.ru
ИНН 5235009307 ОГРН 1235200038347

П Р И К А З

18 августа 2026 года № 9

р.п. Тонкино

Об утверждении Политики парольной защиты для автоматизированных рабочих мест контрольно-счетной комиссии Тонкинского муниципального округа Нижегородской области

В соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» **п р и к а з ы в а ю:**

1. Утвердить прилагаемую Политику парольной защиты для автоматизированных рабочих мест контрольно-счетной комиссии Тонкинского муниципального округа Нижегородской области (далее - Политика).
2. Обеспечить ознакомление сотрудников с Политикой под роспись.
3. Обнародовать настоящий приказ 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 приказа оставляю за собой.

Председатель КСК Тонкинского
муниципального округа Нижегородской области В.М. Халявина

УТВЕРЖДЕНА
распоряжением администрации
Тонкинского муниципального округа
Нижегородской области
от 18.08.20206г № 9

ПОЛИТИКА
парольной защиты для автоматизированных рабочих мест контрольно-счетной комиссии Тонкинского муниципального округа Нижегородской области

1. Общие положения

1.1. Настоящая Политика определяет обязательные требования к минимальным характеристикам и защите паролей учетных записей пользователей на автоматизированных рабочих местах (далее - АРМ) в контрольно-счетной комиссии Тонкинского муниципального округа Нижегородской области.

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 контрольно-счетной комиссии, включая мобильные устройства доступа.

1.4. Требования Политики распространяются как на стандартные пользовательские учетные записи.

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 неизмененном 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.

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 (OTP-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.