



П Р И К А З

30.03.2026

№ 97

О мерах по повышению уровня защищенности информационных ресурсов

С целью повышения уровня защищенности информационных ресурсов и в соответствии с Методикой оценки показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденной ФСТЭК России 11.11.2025 г.,

ПРИКАЗЫВАЮ:

1. Изложить ПРИЛОЖЕНИЕ А Положения по технической защите информации, утвержденного приказом Томского НИМЦ от 09.01.2023г. № 1/3, согласно Приложению.
2. Начальнику отдела информационной безопасности М.С. Колбасу реализовать в информационной инфраструктуре Томского НИМЦ политики идентификации и аутентификации с учетом вносимых изменений в срок до 31.03.2026 года.
3. Контроль исполнения настоящего приказа оставляю за собой.

Директор

В.А. Степанов

Приложение А
к Положению по технической
защите информации

Политики идентификации и аутентификации

№ п/п	Наименование политики	Требуемое значение
1	Запрет повторного использования идентификатора пользователя в течение:	не менее 1 года
2	Длина пароля пользователей:	не менее 12 символов
3	Длина пароля администраторов:	не менее 15 символов
4	Алфавит пароля:	должен содержать буквы верхнего и нижнего регистра (А-Я, А-Z, а-я, а-z), специальные символы (!, », №, %, *, /) и не должно быть персонифицированной информации (имен, адресов, даты рождения, телефонов)
5	Максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки:	от 3 до 10 попыток
6	Блокировка программно-технического средства или учётной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации:	от 5 до 15 минут
7	Период действия паролей:	не более 180 дней
8	Запрет на использование числа последних использованных паролей при создании новых паролей:	не менее 3 последних паролей
9	Задание минимального количества изменённых символов при создании новых паролей:	не менее 12 символов
10	Блокирование сеанса доступа пользователя после времени бездействия (неактивности) пользователя:	не более 15 минут