Совет депутатов Вачского муниципального округа Нижегородской области

РАСПОРЯЖЕНИЕ

от 29.06.2026 г. № 35-х

Об утверждении Положения о требованиях к парольной политике администраторов и пользователей автоматизированных рабочих мест (АРМ) Совета депутатов Вачского муниципального округа Нижегородской области

В соответствии с Федеральным законом от 27.06.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», в целях исполнения требований приказа министерства цифрового развития и связи Нижегородской области от 02.06.2026 №324-62-од «Об утверждении мероприятий по защите информации при подключении абонентов к региональной государственной информационной системе «Система электронного документооборота Нижегородской области, а также в целях совершенствования системы защиты информации в Совете депутатов Вачского муниципального округа Нижегородской области:

1. Утвердить Положение о требованиях к парольной политике администраторов и пользователей автоматизированных рабочих мест (АРМ) Совета депутатов Вачского муниципального округа Нижегородской области.

2. Ответственному за организацию мероприятий по защите информации, обрабатываемой с использованием автоматизированного рабочего места в Совете депутатов Вачского муниципального округа Нижегородской области обеспечить ознакомление муниципальных служащих и работников, замещающих должности, не являющиеся должностями муниципальной службы, на основании трудового договора, иных субъектов персональных данных с данным Положением.

3. Начальнику отдела Совета депутатов Вачского муниципального округа Нижегородской области Антоновой Н.В. обеспечить размещение Перечня на официальном сайте администрации Вачского муниципального округа Нижегородской в информационно-телекоммуникационной сети «Интернет» в десятидневный срок со дня подписания настоящего распоряжения.

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

5. Контроль за исполнением настоящего распоряжения оставляю за собой.

Председатель Совета депутатов С. Е. Липов

Приложение 1
к распоряжению Совета депутатов
Вачского муниципального округа
Нижегородской области
от 29.06.2026 года № 35-х

ПОЛОЖЕНИЕ
о требованиях к парольной политике администраторов и пользователей автоматизированных рабочих мест (АРМ) Совета депутатов Вачского муниципального округа Нижегородской области

1. Общие положения

1.1. Настоящее Положение организации парольной защиты в Совете депутатов Вачского муниципального округа Нижегородской области (далее – Совет депутатов). устанавливает основные правила парольной защиты и регламентирует организационно-техническое обеспечение генерации, смены и прекращения действия паролей, а также контроль за действиями пользователей локальной вычислительной сети Совета депутатов, муниципальных информационных систем (при наличии), информационных систем персональных данных (при наличии) при работе с паролями.

1.2. Настоящее Положение оперирует следующими основными понятиями:

− Идентификация – присвоение субъектам и объектам доступа уникального и однозначно определяющего их в пределах ИСПДн идентификатора, и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

− ИС – информационная система.

− ИСПДн – информационная система персональных данных.

− Компрометация – факт доступа постороннего лица к защищаемой информации, а также подозрение на него.

− Объект доступа – единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

− Пароль – признак субъекта доступа, предъявляемый совместно с идентификатором субъекта в процессе идентификации.

− Правила доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

− Субъект доступа – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

− Несанкционированный доступ – доступ к информации, нарушающий правила разграничения доступа в ИСПД.

2. Правила генерации, использования, хранения, смены паролей

2.1. Персональные пароли должны генерироваться специальными программными средствами либо задаваться субъектом самостоятельно в соответствии с требованиями данного Положения.

2.2. Длина пароля должна быть не менее 8 символов.

2.3. В составе пароля должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы либо пароль должен представлять собой фразу из нескольких слов.

2.4. Пароль не должен включать в себя:

− легко вычисляемые сочетания символов (имена, фамилии и другие), а также общепринятые сокращения и любые другие данные, которые можно определить исходя из информации о пользователе (даты рождения родственников, клички домашних животных и

подобное);

− номера телефонов, автомобилей;

− персональные данные (ФИО, дата рождения, номер паспорта, номер зачетной книжки, адрес и т.п.);

− последовательности из более чем 2 символов, расположенных рядом на клавиатуре (например, 123, qwe и другие);

Пароль не должен состоять из одного и того же повторяющегося символа либо повторяющейся комбинации из нескольких символов (например, 222999, psqpsq).

Запрещается использование паролей, заданных по умолчанию производителями применяемых программных и аппаратных средств обработки и защиты информации.

2.5. Допускается использование единого пароля для доступа субъекта доступа к различным информационным ресурсам одной ИСПД.

2.6. Правила использования паролей.

При использовании паролей пользователь обязан соблюдать положения должностных инструкций, методических документов по защите информации, а также данного Положения.

Ввод пароля должен осуществляться с учетом регистра, в котором пароль был задан.

При вводе паролей необходимо исключить возможность его просмотра посторонними лицами или техническими средствами (фото-, видеокамеры и другие средства).

Пользователь не имеет права сообщать личный пароль другим пользователям и допускать их к работе в своей учетной записи в ИС.

При утере, компрометации, несанкционированном изменении паролей пользователь обязан своевременно сообщать системному администратору администрации Вачского муниципального округа Нижегородской области (далее – администрация).

2.7. Правила хранения паролей.

При хранении паролей должны быть приняты все возможные меры по минимизации возможности компрометации либо утери пароля.

Запрещается:

записывать пароли в файлах, электронных записных книжках, других электронных носителях информации,

указывать пароли на бумажных и других материальных носителях информации, в том числе на предметах,

Запрещается хранение паролей в ИС в открытом виде.

Хранение пользователем паролей на материальном либо электронном носителе допускается только в личном сейфе владельца пароля, либо в сейфе у руководителя организации.

2.8. Правила смены паролей.

Плановая смена паролей пользователя должна проводиться регулярно и не реже указанных в данном пункте сроков.

В ИС, аттестованных по требованиям безопасности информации, плановая смена паролей пользователей должна проводиться в соответствии с требованиями, указанными в аттестационной и организационно-распорядительной документации на ИС, но не реже 1 раза в 90 дней.

В прочих ИС, в том числе предназначенных для обработки персональных данных, плановая смена паролей пользователей должна проводиться не реже 1 раза в 90 дней.

3. Компрометация и прекращение действия паролей

3.1. В случае компрометации либо утери пароля незамедлительно должна проводиться его внеплановая смена. При этом пользователь обязан обратиться к системному администратору администрации.

Внеплановая смена паролей может проводиться по распоряжению системного

администратора администрации после обнаружения фактов попыток несанкционированного доступа, компрометации пароля, либо других нештатных ситуаций;

При смене пароля новое значение должно отличаться от предыдущего не менее чем в 2 символах;

3.2. Правила прекращения действия паролей.

Прекращение действия пароля возможно при истечении срока его действия, внеплановой смене, утере, либо удалении учетной записи.

В случае прекращения полномочий пользователя, в том числе увольнения, переходе на другую работу, системный администратор в обязательном порядке производит удаление его учетной записи и пароля немедленно после окончания последнего сеанса работы данного пользователя с системой. При окончании или прекращении полномочий пользователей не допускается сохранение или передача другим пользователям их учетных записей и паролей.

Запрещается разглашение паролей после прекращения их действия.

4. Ответственность пользователей при работе с парольной защитой

4.1. Ответственность за организацию парольной защиты возлагается на системного администратора администрации.

4.2. Повседневный контроль за действиями работников Совета депутатов при работе с паролями, соблюдением порядка их смены, хранения и использования, возлагается на ответственное лицо по информационной безопасности.

4.3. Владельцы паролей должны быть ознакомлены с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данному Положению, а также за разглашение парольной информации.

4.4. Ответственность в случае несвоевременного уведомления ответственного за информационную безопасность о случаях утери, кражи, взлома или компрометации паролей возлагается на владельца взломанной учетной записи.