Приложение к приказу
от «8» апреля 2025 г.
№ 106-ОД

Политика
Государственного бюджетного учреждения города Москвы
«Жилищник района Коньково» (ГБУ «Жилищник района Коньково»)
в отношении парольной защиты информационных систем и ресурсов

1. Общие положения

Настоящая политика Государственного бюджетного учреждения города Москвы «Жилищник района Коньково» в отношении парольной защиты информационных систем и ресурсов (далее – Политика) устанавливает общие правила и требования по обеспечению парольной защиты информационных систем и ресурсов и/или ИТ-инфраструктуры, создание, развитие (модернизацию), эксплуатацию которых осуществляет Государственного бюджетного учреждения города Москвы «Жилищник района Коньково» (далее - ГБУ «Жилищник района Коньково»).

2. Термины и определения

Документация по защите информации (ЗИ) – документы, определяющие правила и процедуры, реализуемые оператором ИСиР или ИТ-инфраструктуры для обеспечения защиты информации в ходе их эксплуатации.

Идентификатор – признак субъекта доступа или объекта доступа в виде строки знаков (символов), который используется при идентификации и однозначно определяет (указывает) соотнесенную с ним идентификационную информацию.

ИСиР – информационные системы и ресурсы, создание, развитие (модернизацию), эксплуатацию которых осуществляет префектура.

ИТ-инфраструктура – совокупность программных и аппаратных средств, в том числе автоматизированных рабочих мест, с использованием которых осуществляется реализация возложенных на префектуру государственных функций и полномочий, а также доступ к ИСиР города Москвы.

Объект доступа – единица/компонент ИСиР и/или ИТ-инфраструктуры (файл, техническое средство, узел сети, линия (канал) связи, мобильное устройство, программа, том, каталог, запись, поле записей и иные объекты и т.п.), доступ к которой регламентируется правилами разграничения доступа к ИСиР и/или ИТ-инфраструктуре, и по отношению к которым субъекты доступа выполняют операции.

Администратор – лицо, назначаемое ответственным за управление (администрирование) системой защиты информации в ИСиР и/или ИТ-инфраструктуры распорядительным документом префектуры.

Персонал – лицо, обеспечивающее функционирование ИСиР и/или ИТ-инфраструктуры.

Пользователь – лицо, участвующее в функционировании ИСиР и/или ИТ-инфраструктуры или использующее результаты их функционирования и являющееся обладателем учетной записи в ИСиР и/или ИТ-инфраструктуре.

Привилегированная учетная запись – учетная запись персонала ИСиР и/или ИТ-инфраструктуры в соответствии с установленной ролью, наделяющая обладателя такой учетной записи правами по выполнению операций, касающихся функциональных возможностей по управлению (администрированию) ИСиР и/или ИТ-инфраструктуры и (или) управлению (администрированию) системой защиты ИСиР и/или ИТ-инфраструктуры, в том числе по управлению базами данных, прикладным программным обеспечением, телекоммуникационным оборудованием, автоматизированными рабочими местами, серверами, средствами защиты информации и т.п.

Системная (технологическая) учетная запись – учетная запись, используемая для осуществления доступа к ИСиР и/или ИТ-инфраструктуре программными сервисами (службами, процессами).

Субъект доступа – лицо или единица/компонент ИСиР и/или ИТ-инфраструктуры (файл, техническое средство, узел сети, линия (канал) связи, мобильное устройство, программа, том, каталог, запись, поле записей и иные объекты и т.п.), действия которой по доступу к ресурсам ИСиР и/или ИТ-инфраструктуре регламентируются правилами разграничения доступа.

Учетная запись – совокупность идентификатора, пароля, прав доступа
и привилегий в ИСиР и/или ИТ-инфраструктуре.

Учетная запись суперпользователя (root, Administrator) – учетная запись, предоставляющая ее обладателю права и привилегии на выполнение всех без исключения операций и функций в ИСиР и/или ИТ-инфраструктуре и/или их компонентах.

3. Организация парольной защиты

3.1. При доступе пользователей (персонала) к ИСиР и/или ИТ-инфраструктуре должна использоваться аутентификация по паролю. При применении многофакторной аутентификации одним из фактором аутентификации должен быть пароль. Авторизация пользователей (персонала) в ИСиР и/или ИТ-инфраструктуре должна производиться только после их успешной аутентификации.

3.2. Для генерации и хранения паролей для доступа к ИСиР и/или ИТ-инфраструктуре могут применяться специальные программные средства, как автономные, так и входящие в состав установленных на автоматизированных рабочих местах средства защиты информации. При этом пароли, сгенерированные такими средствами, должны удовлетворять требованиям, указанным в разделе 4 настоящей Политики.

3.3. В ИСиР и/или ИТ-инфраструктуре должна быть реализована

защита обратной связи при вводе пользователем (персоналом) пароля путем исключения отображения для пользователя (персонала) действительного значения пароля и (или) количества вводимых символов пароля. Вводимые символы пароля должны отображаться условными знаками, например «*».

3.4. Количество последовательных попыток введения неверного пароля должно быть строго ограничено. После выполнения установленного в Документации по ЗИ количества неуспешных попыток введения пароля (не более 5 (пяти) попыток) должна выполняться временная блокировка учетной записи не менее чем на 15 минут.

3.5. Пароли, установленные производителем программного обеспечения по умолчанию, подлежат изменению непосредственно после его активации.

3.6. Частные правила, требования и последовательность действий по обеспечению парольной защиты конкретных ИСиР и/или ИТ-инфраструктуры описываются в Документации по ЗИ ИСиР и/или ИТ-инфраструктуры с учетом настоящей Политики.

3.7. Администратор обеспечивает корректную настройку и штатную эксплуатацию функционала ИСиР и/или ИТ-инфраструктуры в соответствии с пунктами 3.1-3.6 настоящей Политики.

4. Качество паролей

4.1. Алфавит пароля должен составлять не менее 70 символов - букв английского и(или) русского алфавита верхнего и нижнего регистра, цифр и специальных символов.

4.2. Минимальная длина пароля должна быть не менее 8 символов для учетных записей пользователей (персонала) и не менее 12 для привилегированных учетных записей.

4.3. Пароль должен включать в себя символы не менее трех различных групп из перечисленных:

- заглавные (прописные) буквы (например: A, B, C);
- строчные буквы (например: a, b, c);
- арабские цифры (например: 1, 2, 3);
- специальные символы (например: !, @, &, *).

4.4. Запрещается использовать в качестве пароля наименование учетной записи или ее производную. Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования ИСиР
и другие), а также общепринятые сокращения и любые другие данные, которые можно определить исходя из информации о пользователе (персонале) (даты рождения родственников, клички домашних животных и подобные).

4.5. Пароль не должен включать в себя последовательности из более чем 2 символов, расположенных рядом на клавиатуре (например, 123, qwe).

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

4.7. Запрещается использование паролей, заданных по умолчанию производителями применяемых программных и аппаратных средств обработки и защиты информации (например, user user, admin admin).

4.8. При смене пароля новое значение должно отличаться от предыдущего не менее чем в 5 символах. Новое значение пароля не должно совпадать с 5 предыдущими значениями паролей для данной учетной записи.

4.9. Требования к качеству паролей системных (технологических) учетных записей, учетных записей суперпользователей (root, Administrator) определяются в отношении конкретных ИСиР и/или ИТ-инфраструктуры в Документации по ЗИ, с учетом требований к длине пароля не менее 20 символов и требований настоящей Политики.

4.10. Администраторы обеспечивают выполнение требований пунктов 4.1-4.9 настоящей Политики.

5. Выдача/изменение паролей пользователей (персонала)

5.1. Генерация пароля может производиться по запросу пользователя (персонала) (в случае утраты или компрометации пароля) или автоматически
(в случае создания учетной записи).

5.2. Пароли пользователей (персонала) должны выдаваться/изменяться:

- при принятии[1] нового работника;
- по истечении срока действия пароля;
- в процессе восстановления доступа;
- при изменении пароля пользователем (персоналом);
- при компрометации пароля;
- другие случаи, требующие выдачи/изменения пароля.

5.3. Изменение паролей пользователей (персонала) может осуществляться в двух режимах:

- плановое изменение пароля;
- внеплановое изменение пароля.

5.4. Плановое изменение паролей в ИСиР и/или ИТ-инфраструктуре должно проводиться в соответствии с требованиями Документации по ЗИ ИСиР и/или ИТ-инфраструктуры, нормативных правовых, правовых актах Российской Федерации, города Москвы, регламентирующих эксплуатацию ИСиР и/или ИТ-инфраструктуры, но не реже:

- 1 раза в 90 дней для учетных записей пользователей (персонала);
- 1 раза в 30 дней для привилегированных учетных записей.

5.5. Внеплановое изменение паролей учетных записей пользователей (персонала) в ИСиР и/или ИТ-инфраструктуре может проводиться по инициативе Администратора, а также лицом, ответственным за информационную безопасность в префектуре при обнаружении фактов

[1] В случае необходимости наличия учетной записи в ИСиР и/или ИТ-инфраструктуре для выполнения должностных обязанностей

попыток несанкционированного доступа, компрометации или возникновения подозрения на компрометацию пароля либо других нештатных ситуаций, в случае прекращения полномочий (увольнение, перевод на другую должность) пользователей (персонала) ИСиР и/или ИТ-инфраструктуры и других случаях, требующих изменения паролей.

Для привилегированных учетных записей внеплановое изменение паролей может также производиться по инициативе Администратора, а также лицом, ответственным за информационную безопасность в префектуре перед значимыми мероприятиями для организации (проведения) которых планируется задействовать функционал ИСиР и/или ИТ-инфраструктуры.

5.6. Во всех случаях выдачи/изменения пароля, за исключением случаев истечения срока действия пароля и изменения пароля пользователем (персоналом), пользователю (персоналу) назначается временный пароль. Временный пароль передается пользователю (персоналу) в соответствии с требованиями раздела 6 настоящей Политики. После чего пользователь (персонал) при первом входе в ИСиР и/или ИТ-инфраструктуру должен изменить временный пароль на постоянный, соответствующий требованиям, установленным разделом 4 настоящей Политики.

5.7. По истечении срока действия пароля пользователь (персонал) обязан произвести изменение пароля в соответствии с требованиями пункта 5.4 настоящей Политики.

5.8. В случае утраты, компрометации (возникновения подозрения на компрометацию) пароля учетной записи пользователя (персонала) должно быть проведено внеплановое изменение его пароля.

5.9. Порядок выдачи/изменения паролей учетных записей пользователей (персонала), системных (технологических) учетных записей, учетных записей суперпользователей (root, Administrator) определяется в Документации по ЗИ.

6. Передача реквизитов доступа

6.1. После завершения процедуры создания учетной записи реквизиты доступа (идентификатор и временный пароль) передаются пользователю (персоналу) безопасным способом, исключающим передачу паролей (в том числе временных) в незащищенном виде.

6.2. Порядок передачи реквизитов доступа определяется в отношении конкретных ИСиР и/или ИТ-инфраструктуры в Документации по ЗИ с учетом требований настоящей Политики.

7. Восстановление доступа

7.1. Восстановление доступа к ИСиР и/или ИТ-инфраструктуре в случае утраты, компрометации (возникновения подозрения на компрометацию) пароля осуществляется в порядке, установленном пунктами 5.6, 5.8, 5.9 настоящей Политики.

7.2. Обладатели привилегированных учетных записей в случае утраты/компрометации пароля, обращаются к своему непосредственному

руководителю, который организует смену пароля и сообщает о данном факте Администратору.

7.3. Порядок восстановления доступа определяется в отношении конкретных ИСиР и/или ИТ-инфраструктуры в Документации по ЗИ с учетом требований настоящей Политики.

8. Требования к конфиденциальности паролей

8.1. Запрещено передавать информацию об используемых паролях третьим лицам. Обладатели учетных записей должны обеспечить конфиденциальность паролей. Запрещается хранение паролей в открытом виде вне сейфов, запираемых шкафов.

8.2. Запрещается разглашение паролей после прекращения их действия.

8.3. Запрещается использование чужих идентификаторов и паролей, а также осуществление их подбора.

9. Контроль

9.1. Администратор на постоянной основе обеспечивает проведение контроля действий пользователей (персонала) ИСиР и/или ИТ-инфраструктуры при работе с паролями.

9.2. Администратор на постоянной основе обеспечивает проведение анализа журналов событий доступа привилегированных учетных записей, системных (технологических) учетных записей, учетных записей суперпользователей (root, Administrator) на предмет попыток неправомерного доступа, и обеспечивает инициирование процедуры изменения пароля в случае подозрения на его компрометацию.

10. Ответственность

10.1. Пользователи (персонал) ИСиР и/или ИТ-инфраструктуры несут персональную ответственность за соблюдение требований к паролям и конфиденциальность паролей к своим учетным записям, установленных настоящей Политикой.

10.2. В случае компрометации пароля к учетной записи пользователи (персонал) ИСиР и/или ИТ-инфраструктуры несут персональную ответственность за все действия, совершенные с использованием их учетной записи, если с их стороны не было предпринято необходимых действий по предотвращению компрометации пароля.

10.3. Лица, участвующие в парольной защите ИСиР и/или ИТ-инфраструктуры, несут персональную ответственность за соблюдение требований настоящей Политики.