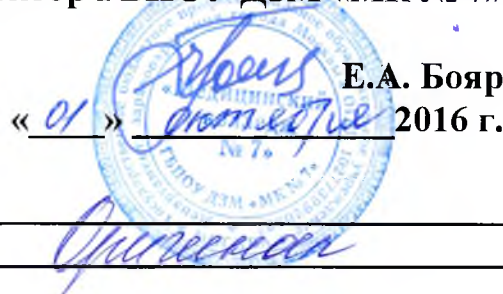


ГБПОУ ДЗМ «МК № 7»	001-10-2016	<b>ПОЛОЖЕНИЕ</b> по организации парольной защиты в ГБПОУ ДЗМ «МК № 7»	Лист 1	Листов 7
-----------------------	-------------	---	-----------	-------------

Рег. № 6

**УТВЕРЖДАЮ**  
Директор ГБПОУ ДЗМ «МК № 7»

Е.А. Бояр  
« 01 » сентября 2016 г.



**ПОЛОЖЕНИЕ**  
по организации парольной защиты  
в ГБПОУ ДЗМ «МК № 7»

**1. Общие положения**

1.1. Данное Положение регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационной системе Государственного бюджетного профессионального образовательного учреждения Департамента здравоохранения города Москвы «Медицинский колледж № 7» (далее – Учреждение), меры обеспечения безопасности при использовании паролей, а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

1.2. Требования настоящего Положения являются неотъемлемой частью комплекса мер безопасности и защиты информации Учреждения.

1.3. Требования настоящего Положения распространяются на всех работников структурных подразделений, использующих в работе средства вычислительной техники, и должны применяться для всех средств вычислительной техники, эксплуатируемой в Учреждении.

1.4. Организационное обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех информационных системах Учреждения и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на руководителя Учреждения.

Техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей возлагается на администратора локальной вычислительной сети (далее - администратор ЛВС) Учреждения.

ГБПОУ ДЗМ «МК № 7»	001-10-2016	<b>ПОЛОЖЕНИЕ</b> по организации парольной защиты в ГБПОУ ДЗМ «МК № 7»	Лист 2	Листов 7
-----------------------	-------------	---	-----------	-------------

1.5. Ознакомление всех работников Учреждения, использующих средства вычислительной техники, с требованиями Положения проводят руководители структурных подразделений. При ознакомлении с Положением внимание работников акцентируется на предупреждении их о персональной ответственности за разглашение парольной информации.

## 2. Термины и определения

**Информационная система (ИС)** - совокупность программных и аппаратных средств, предназначенных для хранения, передачи и обработки данных и информации и производства вычислений.

**Информационная безопасность (ИБ)** - обеспечение защищенности информации (ее конфиденциальности, целостности, доступности) от широкого спектра угроз с целью обеспечения непрерывности процесса и минимизации рисков.

**Учетная запись** - информация о сетевом пользователе: имя пользователя, его пароль, права доступа к ресурсам и привилегии при работе в системе. Учетная запись может содержать дополнительную информацию (адрес электронной почты, телефон и т.п.).

**Принцип минимальных привилегий** - принцип, согласно которому каждому субъекту системы предоставляется минимальный набор полномочий (или минимальный допуск), необходимый для выполнения вверенных задач. Применение этого принципа ограничивает ущерб, наносимый в случае случайного, ошибочного или несанкционированного использования.

**Компрометация** - утрата доверия к тому, что информация недоступна посторонним лицам.

**Ключевой носитель** - электронный носитель (дискета, флэш-накопитель, компакт-диск и т.п.), на котором находится ключевая информация (сертификаты и т.п.).

## 3. Общие требования к паролям

3.1. Пароли доступа ко всем информационным ресурсам первоначально формируются администратором ЛВС, а в дальнейшем выбираются пользователями самостоятельно, но с учетом требований, изложенных ниже.

3.2. Личные пароли пользователей автоматизированной системы Учреждения должны выбираться с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы, цифры и (или) специальные символы (@, #, \$, &, \*, % и т.п.);

ГБПОУ ДЗМ «МК № 7»	001-10-2016	<b>ПОЛОЖЕНИЕ</b> по организации парольной защиты в ГБПОУ ДЗМ «МК № 7»	Лист 3	Листов 7
-----------------------	-------------	---	-----------	-------------

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования рабочих станций и т.д.), а также общепринятые сокращения и термины (qwerty, p@ssw0rd и т.п.);

- при смене пароля новый пароль должен отличаться от старого не менее чем двумя символами.

3.3. Пароли служебных и привилегированных учетных записей автоматизированной системы должны выбираться с учетом следующих требований:

- длина пароля должна быть не менее 12 символов;
- в числе символов пароля обязательно должны присутствовать цифры и (или) специальные символы (@, #, \$, &, \*, %, и т.п.);

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования рабочих станций и т.д.), а также общепринятые сокращения и термины (qwerty, p@ssw0rd и т.п.), пароль не должен быть словом русского либо английского языка, в котором заменены некоторые символы (o->0, s->\$, a->@ и т.п.);

- при смене пароля новый пароль должен отличаться от старого не менее чем четырьмя символами, расположенными подряд;

- при создании паролей служебных учетных записей возможно использование специализированного программного обеспечения для генерации сложных для подбора легко запоминаемых паролей.

#### **4. Безопасность локальных учетных записей**

4.1. Локальные учетные записи компьютеров (Administrator, Guest) предназначены для служебного использования администратором ЛВС при настройке систем и не предназначены для повседневной работы.

4.2. Создание и использование локальных учетных записей на рабочих станциях, подключенных к ИС Учреждения и входящих в состав домена, пользователям запрещено.

4.3. Встроенная учетная запись Guest (Гость) должна быть заблокирована на всех рабочих станциях в составе ИС Учреждения при первоначальном конфигурировании операционной системы.

4.4. Встроенная учетная запись Administrator (Администратор) должна быть защищена паролем согласно п. 3.3 настоящего Положения.

4.5. BIOS рабочих станций в составе ИС Учреждения должна быть защищена паролем согласно п. 3.3 настоящего Положения.

#### **5. Безопасность доменных учетных записей**

5.1. Пользователь несет персональную ответственность за сохранение в тайне личного пароля. Запрещается сообщать пароль другим лицам, а также хранить записанный пароль в общедоступных местах.

ГБПОУ ДЗМ «МК № 7»	001-10-2016	ПОЛОЖЕНИЕ по организации парольной защиты в ГБПОУ ДЗМ «МК № 7»	Лист 4	Листов 7
-----------------------	-------------	--	-----------	-------------

5.2. В случае производственной необходимости (командировка, отпуск и т.п.) при проведении проверочных мероприятий, требующих знания пароля пользователя, допускается раскрытие значений своего пароля руководителям этих структурных подразделений. По окончании производственных или проверочных работ работники самостоятельно производят немедленную смену значений «раскрытых» паролей.

5.3. В случае возникновения нештатных ситуаций, форс-мажорных обстоятельств, а также технологической необходимости использования имен и паролей работников (в их отсутствие) допускается изменение паролей администратором ЛВС. В подобных случаях работники, чьи пароли были изменены, обязаны сразу же после выяснения факта смены своих паролей создать их новые значения.

5.4. Пароли учетных записей пользователей ИС Учреждения должны соответствовать требованиям п. 3.2 настоящего Положения.

5.5. К управлению доменными учетными записями пользователей необходимо подходить исходя из принципа «минимальных привилегий», т.е. пользователь не должен иметь прав доступа как к локальной системе, так и к ресурсам ИС Учреждения больше, чем это необходимо ему для выполнения своих должностных обязанностей.

5.6. Полная плановая смена паролей пользователей должна проводиться регулярно не реже одного раза в 2 месяца. Плановая смена должна предусматривать информирование пользователя о необходимости сменить пароль и возможность смены пароля без обращения к администратору сети.

5.7. Внеплановая смена личного пароля или удаление учетной записи пользователя информационной системы в случае прекращения его полномочий (увольнение и т.п.) должна производиться администратором ЛВС немедленно после окончания последнего сеанса работы данного пользователя с системой.

5.8. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на работу в другое подразделение внутри Учреждения и другие обстоятельства) администратора ЛВС и других работников, которым по роду работы были предоставлены полномочия по управлению парольной защитой ИС Учреждения.

5.9. В случае компрометации личного пароля пользователя ИС Учреждения либо подозрения на компрометацию должны быть немедленно предприняты меры по внеплановой смене личного пароля самим пользователем.

5.10. Смена забытого пользовательского пароля производится администратором ЛВС на основании сообщения пользователя с обязательной установкой параметра «Требовать смену пароля при следующем входе в систему».

ГБПОУ ДЗМ «МК № 7»	001-10-2016	<b>ПОЛОЖЕНИЕ</b> по организации парольной защиты в ГБПОУ ДЗМ «МК № 7»	Лист 5	Листов 7
-----------------------	-------------	---	-----------	-------------

5.11. Для предотвращения угадывания паролей администратор ЛВС обязан настроить механизм блокировки учетной записи на 20 минут при пятикратном неправильном вводе пароля.

5.12. При временном оставлении рабочего места в течение рабочего дня рабочая станция в обязательном порядке блокируется нажатием комбинации клавиш "Win + L".

5.13. При возникновении вопросов, связанных с использованием доменных учетных записей, пользователь ИС Учреждения обязан обратиться к администратору ЛВС Учреждения.

## **6. Временные учетные записи**

6.1. Для предоставления временного доступа к ресурсам ИС Учреждения лицам, не являющимся сотрудниками Учреждения, необходимо использовать процедуру временных учетных записей.

6.2. Временная учетная запись - учетная запись, имеющая ограничение по времени действия.

6.3. Порядок получения, продления в случае необходимости временных учетных записей определяется в Положении о регистрации пользователей информационных систем Учреждения.

## **7. Безопасность служебных и привилегированных учетных записей**

7.1. К служебным учетным записям относятся учетные записи, используемые структурными подразделениями либо техническим персоналом ИС Учреждения для доступа к ресурсам, необходимым для выполнения их функций. К привилегированным учетным записям относятся учетные записи, используемые для управления работой ИС Учреждения.

7.2. При использовании привилегированных учетных записей (администратора) необходимо руководствоваться принципом «минимальных привилегий», т.е. привилегии администратора должны использоваться только администратором и только если выполняемая задача требует наличия таких привилегий.

7.3. Использование привилегированных учетных записей в повседневной работе, не связанной с необходимостью их использования (установка, конфигурирование, восстановление и т.п. операционной системы и сервисов), недопустимо, в случае необходимости запуска программы с правами Администратора пользователь обязан использовать команду «Run As...» либо «вторичный вход в систему».

7.4. Учетная запись администратора домена должна использоваться только при установке, конфигурировании, восстановлении контроллера домена и иных действиях, при которых использование других учетных

ГБПОУ ДЗМ «МК № 7»	001-10-2016	<b>ПОЛОЖЕНИЕ</b> по организации парольной защиты в ГБПОУ ДЗМ «МК № 7»	Лист 6	Листов 7
-----------------------	-------------	---	-----------	-------------

записей невозможно. Для этой учетной записи необходимо подробное протоколирование всех событий ее использования, а также немедленное расследование любого нецелевого ее использования.

7.5. Использование принципа «минимальных привилегий» необходимо для служб и сервисов, выполняющихся на серверах ИС Учреждения, т.е. службы и сервисы должны работать с минимально возможными для их корректной работы привилегиями исходя из следующей иерархии:

- локальная служба;
- сетевая служба;
- уникальная учетная запись локального пользователя;
- уникальная учетная запись пользователя домена;
- локальная система;
- учетная запись локального администратора;
- учетная запись администратора домена.

7.6. К серверам высокой степени безопасности (контроллеры домена, серверы баз данных, иные серверы, от которых зависит бесперебойная работа ИС Учреждения) необходимо предъявлять повышенные требования к минимизации привилегий доступа со стороны как удаленных, так и локальных пользователей и служб.

7.7. В случае компрометации либо подозрения на компрометацию привилегированной учетной записи необходима внеплановая смена паролей всех зависящих от нее учетных записей.

## 8. Контроль

8.1. Повседневный контроль над соблюдением требований данного Положения заключается в контроле процессов использования и изменения учетных записей, процессов доступа к ресурсам, процессов изменения учетных записей и предоставления доступа к ресурсам ИС Учреждения администратором ЛВС Учреждения.

8.2. Администратор ЛВС Учреждения проводит ежеквартальный выборочный контроль выполнения работниками Учреждения требований Положения. О фактах несоответствия качества паролей или условий обеспечения их сохранности сообщается руководителю Учреждения в форме служебной записки.

## 9. Ответственность

9.1. Пользователи ИС Учреждения несут персональную ответственность за несоблюдение требований по парольной защите.

9.2. Администратор ЛВС несет ответственность за компрометацию и нецелевое использование привилегированных учетных записей.

ГБПОУ ДЗМ «МК № 7»	001-10-2016	<b>ПОЛОЖЕНИЕ</b> по организации парольной защиты в ГБПОУ ДЗМ «МК № 7»	Лист 7	Листов 7
-----------------------	-------------	---	-----------	-------------

9.3. Форма и размер ответственности определяются исходя из вида и размера ущерба, нанесенного ресурсам ИС Учреждения действиями либо бездействием соответствующего пользователя.

Разработано:  
Программист

А.А. Таренко

Согласовано:  
Начальник отдела кадрового  
и правового обеспечения

И.В. Головина