
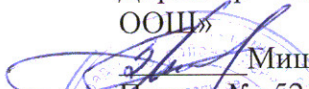
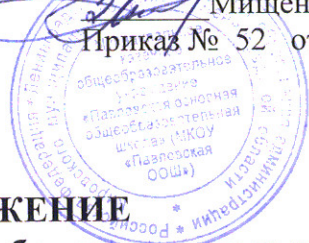


Согласовано:  
Председатель СТК  
 Лобанова Е.Г.  
Протокол № 13 от  
24.04.13

Утверждено:  
Директор МКОУ «Павловская  
ООШ»

  
Мищенко З.П.  
Приказ № 52 от 26.04.13



## **ПОЛОЖЕНИЕ**

### **о парольной защите при обработке персональных данных и иной конфиденциальной информации в МКОУ «Павловская ООШ»**

#### **I. Общие положения**

##### **1.1. Введение**

Данное Положение регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в информационных системах (ИС) организации, а также контроль за действиями Пользователей и обслуживающего персонала при работе с паролями в МКОУ «Павловская ООШ» (далее – ОУ). Парольная защита требует соблюдения ряда правил, изложенных в настоящем Положении.

##### **1.2. Цель**

Положение определяет требования ОУ к парольной защите информационных систем.

##### **1.3. Область действия**

Положение распространяется на всех пользователей и информационные системы (далее – ИС) ОУ, использующих парольную защиту.

#### **II. Термины и определения**

ИС – в данном случае любая информационная система, для работы с которой необходима аутентификация пользователя.

Пароль – секретный набор символов, используемый для аутентификации пользователя. Пользователи – администраторы ИС и работники Общества или сторонней организации, которым предоставлен доступ к ИС Общества, а также корпоративный доступ к ресурсам сети Интернет.

Учетная запись – идентификатор пользователя, используемый для доступа к ИС.

### **III. Положения**

3.1. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями ИС самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;
- личный пароль Пользователь не имеет права сообщать никому.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

3.2. При наличии технологической необходимости (в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п.) использования имен и паролей некоторых сотрудников (Пользователей) в их отсутствие, такие сотрудники обязаны сразу же после смены своих паролей сообщать руководителю их новые значения.

3.3. Внеплановая смена личного пароля или удаление учетной записи Пользователя ИС в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться сотрудниками, отвечающими за работу ИС немедленно после окончания последнего сеанса работы данного Пользователя с системой.

3.4. Внеплановая полная смена паролей всех Пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) администраторов средств защиты и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой ИС.

3.5. Хранение Пользователем своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у руководителя в опечатанном конверте.

3.6. Повседневный контроль за действиями Пользователей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования, возлагается на сотрудников инженерной службы МКОУ «Павловская ООШ».

### **IV. Роли и ответственность**

4.1. Пользователи:

4.1.1. Исполняют требования положения и несут ответственность за ее нарушение.

4.1.2. Информировывают администратора парольной защиты обо всех ставших им известных случаях нарушения настоящего положения.

4.2. Администратор парольной защиты:

4.2.1. Принимает обращения пользователей по вопросам парольной защиты (например, блокировка четных записей, нарушение положения и др.).

4.2.2. Организует консультации пользователей по вопросам использования парольной защиты.

4.2.3. Контролирует действия Пользователей при работе с паролями, соблюдением порядка их смены, хранения и использования.

4.2.4. Отвечает за безопасное хранение паролей встроенных административных учетных записей.