Приложение № 1
к приказу МБУДО ДШИ № 28
№ 43/1-од от 25.05.2017г.

Директор /В.К. Мартынюк

ПОЛОЖЕНИЕ
по организации парольной защиты в информационных системах муниципального бюджетного учреждения дополнительного образования города Новосибирска «Детская школа искусств № 28»

Глава 1. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящее Положение регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах муниципального бюджетного учреждения дополнительного образования города Новосибирска «Детская школа искусств № 28» (далее - ИС), требования к содержанию паролей, а также контроль за действиями пользователей информационных систем при работе с идентификаторами и персональными паролями.

2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в ИС и контроль за данными действиями возлагается на администратора информационных систем.

3. Контроль за действиями пользователей в ИС при работе с паролями, соблюдением порядка их смены, хранения и за соответствие паролей требованиям настоящего Положения возлагается на сотрудника, ответственного за организацию обработки персональных данных.

Глава 2. ПРАВИЛА ФОРМИРОВАНИЯ ПАРОЛЕЙ

4. Персональные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями информационных систем самостоятельно с учетом следующих требований:

а) длина пароля должна быть не менее 6 символов;

б) в числе символов пароля рекомендуется присутствие букв в верхнем и нижнем регистрах, цифр;

в) пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, abcd и т.д.),

общепринятые сокращения (ADMIN, SECRET, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетания букв и знаков, которые можно угадать, основываясь на информации о пользователе;

г) использование трех и более подряд идущих на клавиатуре символов, набранных в одном регистре, недопустимо;

д) при смене пароля новое значение должно отличаться от предыдущего не менее чем в 3 позициях;

е) личный пароль пользователь не имеет права сообщать никому;

ж) новый пароль не должен совпадать с одним из трех предыдущих паролей;

з) пользователь обязан сохранять в тайне свой личный пароль.

5. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на администратора информационных систем.

6. При технологической необходимости использования учетных данных некоторых работников в их отсутствие (в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п.) администратором информационных систем по письменному запросу заинтересованного лица, содержащего разрешение руководителя учреждения, предоставляется одноразовый пароль на данную учетную запись. По возвращении работник обязан сменить персональный пароль на все локальное программное обеспечение.

Глава 3. ВВОД ПАРОЛЯ

7. В целях обеспечения информационной безопасности и противодействия попыткам подбора пароля в ИС определены правила ввода пароля:

а) символы вводимого пароля не отображаются на экране в явном виде;

б) учет всех попыток (успешных и неудачных) входа в систему.

8. При первоначальном вводе или смене пароля пользователя действуют следующие правила:

а) символы вводимого пароля не должны явно отображаться на экране;

б) для подтверждения правильности ввода пароля (с учетом первого правила) - ввод пароля необходимо проводить 2 раза.

9. Ввод пароля должен осуществляться непосредственно пользователем ИС (владельцем пароля). Пользователю запрещается передавать пароль для ввода другим лицам. Передача пароля для ввода другим лицам является разглашением конфиденциальной информации и влечет за собой ответственность в соответствии с действующим законодательством Российской Федерации.

10. Непосредственно перед вводом пароля для предотвращения возможности неверного ввода пользователь ИС должен убедиться в правильности языка ввода (раскладки клавиатуры), проверить, не является ли активной клавиша CAPS LOCK (если это необходимо), а также проконтролировать расположение клавиатуры (клавиатура должна располагаться таким образом, чтобы исключить возможность увидеть набираемый текст посторонними).

11. При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его подсматривания посторонними лицами и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т.п.).

Глава 4. ПОРЯДОК СМЕНЫ ЛИЧНЫХ ПАРОЛЕЙ

12. Полная плановая смена паролей проводится регулярно, не реже одного раза в течение одного учебного года.

13. При смене пароля администратором информационныхсистем производится тестирование функций средств защиты информации от несанкционированного доступа путем ввода с клавиатуры заведомо ложного пароля, при наличии считывателя - предъявления стороннего идентификатора.

14. Внеплановая смена персонального пароля или удаление учетной записи пользователя ИС в случае прекращения его полномочий (увольнение, переход на другую работу внутри учреждения и т.п.) должны производиться

администратором информационныхсистем немедленно после окончания последнего сеанса работы данного пользователя с системой.

15. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри учреждения и т.д.) администратора информационныхсистем, работника, ответственного за организацию обработки персональных данных и других работников, которым для выполнения их должностных обязанностей были предоставлены полномочия по управлению парольной защитой подсистем ИС.

16. Временный пароль, заданный администратором информационных систем при регистрации нового пользователя, следует изменить при первом входе в систему.

17. Учетная запись пользователя, ушедшего в длительный отпуск (более 60 дней), должна блокироваться администратором информационных систем.

18. Удаление учетных записей пользователей, уволенных, переведенных в другое структурное подразделение, филиал, должно производиться администратором информационных систем немедленно.

Глава 5. ХРАНЕНИЕ ПАРОЛЯ

19. Хранение пароля должно обеспечивать его сохранность и недоступность посторонним лицам.

20. Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

Глава 6. ДЕЙСТВИЯ В СЛУЧАЕ УТЕРИ И КОМПРОМЕТАЦИИ ПАРОЛЯ

21. В случае возникновения необходимости в смене пароля ввиду компрометации пользователь должен:

а) немедленно сменить свой пароль;

б) известить администратора информационных систем;

в) известить работника, ответственного за организацию обработки персональных данных в учреждении.

22. В случае компрометации (утеря, передача парольной информации) персонального пароля пользователя ИС должны быть немедленно предприняты меры в соответствии с пунктом 14 или пунктом 15 настоящего Положения в зависимости от полномочий владельца скомпрометированного пароля.

Глава 7. ОТВЕТСТВЕННОСТЬ ПРИ ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ

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

24. Ответственность за организацию парольной защиты в ИС возлагается на администратора информационных систем.

25. Лица, имеющие отношение к обработке персональных данных в ИС, должны быть ознакомлены с настоящим Положением под расписку.