

11

ОТДЕЛ ОБРАЗОВАНИЯ  
АДМИНИСТРАЦИИ ВАРГАШИНСКОГО РАЙОНА

ПРИКАЗ

от 10 апреля 2017 года

№ 31

Об утверждении инструкции по организации парольной защиты  
в информационной системе персональных данных Отдела образования  
Администрации Варгашинского района

Во исполнение Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановления Правительства РФ от 01 ноября 2012 года №1119 «О утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 года №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» ПРИКАЗЫВАЮ:

1. Утвердить инструкцию по организации парольной защиты в информационной системе Отдела образования Администрации Варгашинского района (далее – Инструкция).
2. Ответственным за организацию и обеспечение парольной защиты в информационной системе персональных данных Отдела образования Администрации Варгашинского района назначить системного администратора.
3. Контроль за выполнением приказа возложить на начальника службы организационно-правовой и кадровой работы Отдела образования Администрации Варгашинского района.

Начальник Отдела образования  
Администрации Варгашинского района

*Кожево*

С.А. Кожева

С приказом ознакомлен:

*Дорофеев* П.С. Дорофеев

13

Приложение к приказу  
Отдела образования  
Администрации Варгашинского района  
от \_\_\_\_\_ № \_\_\_\_\_  
«Об утверждении инструкции по  
организации парольной защиты  
в информационной системе  
Отдела образования Администрации  
Варгашинского района»

**Инструкция  
по организации парольной защиты в  
информационной системе Отдела образования Администрации  
Варгашинского района**

**I. ОБЩИЕ ПОЛОЖЕНИЯ**

1. Настоящая инструкция разработана в соответствии с Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом Федеральной службы по техническому и экспортному контролю России от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», а также другими нормативными правовыми актами по защите информации, и регламентирует процессы генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах персональных данных (далее – ИСПДн) Отдела образования Администрации Варгашинского района (далее – Отдел образования), а также контроль над действиями пользователей системы при работе с паролями.

2. Осуществление процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями исполнителей системы при работе с паролями возлагается на администратора безопасности ИСПДн.

**II. ПРАВИЛА ФОРМИРОВАНИЯ ПАРОЛЕЙ**

3. Личные пароли пользователей ИСПДн Отдела образования (далее – пользователей) должны генерироваться и распределяться централизованно либо

выбираться пользователями информационной системы самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 6 символов;
- в числе символов пароля обязательно присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, \$, &, \*, % и т.п.);
- пароль не должен включать в себя имя пользователя, легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, абвгд и т.д.), общепринятые сокращения (ЭВМ, ЛВС, 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;
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в шести позициях.

4. Пользователям допускается использовать пароли, составленные из первых букв слов запоминающихся высказываний в разном регистре, смешанные в произвольном порядке со специальными символами (например Кожзгсф7!).

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

6. Для обеспечения возможности использования имен и паролей некоторых пользователей в их отсутствие (например, в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п.), пользователи обязаны сразу же после установки своих паролей передавать их на хранение вместе с именами своих учетных записей администратору безопасности ИСПДн в запечатанном конверте или опечатанном пенале. Опечатанные конверты (пеналы) с паролями пользователей должны храниться в опечатанном сейфе, к которому исключен доступ других пользователей посторонних лиц. Для опечатывания конвертов (пеналов) должна применяться печать для документов Отдела образования Администрации Варгашинского района. Все конверты (пеналы) с паролями в обязательном порядке фиксируются в «Журнале учета паролей пользователей...».

### **III. ВВОД ПАРОЛЯ**

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

8. При неверном вводе пароля более 5 раз, учетная запись пользователя должна блокироваться не менее чем на 3 минуты и не более чем на 15 минут.

### **IV. ПОРЯДОК СМЕНЫ ЛИЧНЫХ ПАРОЛЕЙ**

9. Смена паролей должна проводиться регулярно, не реже одного раза в 6 месяцев, самостоятельно каждым пользователем.

В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т.п.) должно производиться немедленное удаление его учетной записи сразу после окончания последнего сеанса работы данного пользователя с системой.

10. Срочная (внеплановая) полная смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) ответственного за обеспечение безопасности персональных данных, администратора безопасности и других пользователей, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

11. Администратор безопасности ИСПДн ведет «Журнал учета паролей пользователей...», в котором он отмечает причины внеплановой смены паролей пользователей.

12. Временный пароль, заданный администратором безопасности ИСПДн при регистрации нового пользователя, должен действовать в течение ограниченного срока времени. Пользователь должен изменить временный пароль при первом входе в систему.

## **V. ХРАНЕНИЕ ПАРОЛЯ**

13. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке, мобильном телефоне и любых других предметах и носителях информации.

14. Запрещается сообщать свой пароль полностью или частично другим пользователям, запрещается спрашивать или подсматривать пароль других пользователей.

15. Запрещается регистрировать других пользователей в ИСПДн со своим личным паролем, запрещается входить в ИСПДн под учетной записью и паролем другого пользователя.

## **VI. ДЕЙСТВИЯ В СЛУЧАЕ УТЕРИ И КОМПРОМЕТАЦИИ ПАРОЛЯ**

16. В случае утери или компрометации (разглашения, утраты) или подозрения в компрометации пароля пользователя должна быть немедленно проведена внеплановая процедура смены пароля.

## **VII. ОТВЕТСТВЕННОСТЬ**

17. Каждый пользователь ИСПДн несет персональную ответственность за соблюдение требований настоящей Инструкции и за все действия, совершенные от имени его учетной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения компрометации пароля его учетной записи.

18. Ответственность за контроль проведения мероприятий по организации парольной защиты в структурных подразделениях Отдела образования возлагается на ответственного за обеспечение безопасности персональных данных.

19. За разглашение персональных данных и нарушение порядка работы со средствами ИСПДн, обрабатывающими персональные данные, работники могут

быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности в установленном законом порядке.