|  |  |
| --- | --- |
|  | Приложение 8  к приказу руководителя *Организации*  от \_\_ №\_\_\_\_ |

Инструкция по применению парольной защиты и личных идентификаторов

в информационных системах персональных данных

*Организации*

1. Настоящая инструкция определяет требования к порядку использования, генерации, смены и прекращения действия паролей и личных идентификаторов пользователей в информационных системах персональных данных в *Организации* (далее – ИСПДн) и устанавливает ответственность сотрудников *Организации*, эксплуатирующих и сопровождающих ИСПДн, за их выполнение, а также к контролю действий пользователей при работе с паролями.
2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей, а также контроль действий пользователей при работе с паролями возлагается на администратора информационной безопасности в *Организации* (далее - АИБ).
3. Пароли для всех учетных записей пользователей ИСПДн должны выбираться с учетом следующих требований:
4. длина пароля должна быть не менее 6 буквенно-цифровых символов;
5. пароль не должен включать в себя легко вычисляемые (угадываемые) сочетания символов (имена, фамилии, отчества, наименования в *Организации* и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER, ADM, ADMIN и т.п.);
6. максимальное действие пароля - не более чем 90 дней;
7. пароль не должен повторяться;
8. пользователь не может неправильно ввести пароль учетной записи более 5 раз, в этом случае должна происходить блокировка учетной записи пользователя, до момента снятия блокировки.
9. Для генерации «стойких» значений паролей могут применяться специальные программные средства.
10. При первичной регистрации пользователя в ИСПДн пароль ему назначает АИБ.
11. Пользователи ИСПДн обязаны хранить свой личный пароль втайне от других и не передавать любым способом пароль третьим лицам.
12. Пользователь ИСПДн лично должен проводить смену пароля учетной записи регулярно не реже одного раза в три месяца.
13. Привязку идентификатора к пользователю (учетной записи) выполняет АИБ.
14. Пользователи ИСПДн получают свой идентификатор у АИБ.
15. Пользователь ИСПДн обязан хранить свой личный идентификатор в недоступных для других сотрудников хранилищах.
16. Пользователю ИСПДн запрещается передавать свой личный идентификатор.
17. В случае утери личного идентификатора, пользователь ИСПДн должен немедленно доложить об этом АИБ.
18. При наличии технологической необходимости использования имен и паролей сотрудников в их отсутствие (например, в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п.), пароли данных сотрудников должны быть незамедлительно изменены АИБ.
19. Полная плановая смена паролей пользователей должна проводиться регулярно, но не реже одного раза в год.
20. В случае прекращения полномочий пользователя ИСПДн (увольнение, переход на другую работу, в другой отдел или помещение, а также другие обстоятельства) учетная запись должна быть удалена, а её идентификатор должен быть сдан АИБ после окончания последнего сеанса работы данного пользователя в ИСПДн.
21. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и другие обстоятельства) АИБ.
22. В случае компрометации личного пароля или утери личного идентификатора пользователя АИБ должны быть немедленно предприняты меры в соответствии с пунктом 18 настоящей Инструкции.
23. АИБ должен провести служебное расследование для выяснения причин компрометации пароля с целью выработки новых или совершенствования принятых технических и организационных мер по устранению такой угрозы в будущем, а также выяснению величины ущерба, который может быть нанесен собственнику информационных ресурсов.
24. Доведение Инструкции до сотрудников *Организации* в части их касающейся осуществляется АИБ под роспись в листе ознакомления с данной инструкцией.