

УТВЕРЖДАЮ
Ректор АОУ ВО ДПО «Вологодский
институт развития образования»



И.А. Макарьина

«23» апреля 2018 г.

ИНСТРУКЦИЯ
по организации парольной защиты
информационных систем персональных данных
в автономном образовательном учреждении Вологодской области
дополнительного профессионального образования «Вологодский институт
развития образования»

Данная инструкция регламентирует действия пользователей при работе с паролями.

1. Идентификация и проверка подлинности пароля при входе в информационную систему персональных данных (далее – ИСПДн) осуществляется по паролю условно-постоянного действия.

2. Процесс генерации, использования, смены и прекращения действия пароля для администрирования системы возлагается начальника отдела информационно-коммуникационных технологий. Начальник отдела информационно-коммуникационных технологий должен быть включен в список лиц, допущенных к обработке персональных данных.

3. Личные пароли генерируются первоначально централизованно с последующей заменой пользователем на рабочем месте. Личный пароль пользователь не имеет права кому-либо сообщать.

4. Пароли генерируются специализированными программами или создаются с учетом следующих требований:

- длина пароля не должна быть менее шести буквенно-цифровых символов;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования рабочих мест, словарные и жаргонные слова и т.д.), общепринятые сокращения (USER и т.п.), последовательности символов и знаков (111, qwerty, abcdef, 123456, 098765 и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях.

5. Полная плановая смена паролей должна проводиться регулярно 1 раз в месяц.

6. Плановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться немедленно после окончания последнего сеанса работы данного пользователя с системой.

7. В случае компрометации (утраты, разглашения, кражи, взлома) личного пароля пользователь ИСПДн должен немедленно предпринять меры в соответствии с п. 6 настоящей Инструкции.

8. Хранение пользователем значений своих паролей на материальном носителе допускается только в личном, запираемом ящике (сейфе).

9. Список паролей пользователей ИСПДн должен храниться в опечатанном конверте или пенале у ответственного за обеспечение безопасности ИСПДн, либо у руководителя подразделения.

Этот список может использоваться при технологической необходимости использования имен и паролей некоторых работников в их отсутствие (в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п.)

После использования работник, чей пароль был использован, обязан сразу после выхода на рабочее место сменить пароль на новые значения и передать на хранение лицу, указанного в первом абзаце данного пункта.

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

11. 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 информации о пароле.

12. Контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены и использования в подразделениях возлагается на начальника отдела информационно-коммуникационных технологий.