

УТВЕРЖДАЮ

Председатель кооператива ЖКС  
Энергетик Золотов Ю.Ю. Золотов



«07» января 2018 г.

✓ 6

**ИНСТРУКЦИЯ ПО ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ  
информационных систем персональных данных  
кооператива ЖКС «Энергетик»**

2018 г.

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в информационных системах персональных данных (далее – ИСПДн) кооператива ЖКС «Энергетик» (далее – Кооператив), а также контроль за действиями пользователей ИСПДн при работе с паролями.

1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями пользователей при работе с паролями возлагается на администратора информационной безопасности.

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

- длина пароля должна быть не менее 6 (шести) символов;
- в числе символов пароля **обязательно должны присутствовать** буквы в верхнем или нижнем регистрах, цифры и/или специальные символы (@, #, \$, &, \*, % и т.п.);
- символы паролей для рабочей станции должны вводиться в режиме латинской раскладки клавиатуры;
- 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.

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. В случае замещения основных сотрудников (исполнителей) в связи с отпуском или больничным, возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п. администратор информационной безопасности может воспользоваться именем и паролем отсутствующего сотрудника (исполнителя), либо передать имя и пароль лицу, заменяющего отсутствующего сотрудника (исполнителя), и возложить на него в письменном виде (в произвольной форме) ответственность за сохранность и неразглашение конфиденциальной информации. По возвращении сотрудника (исполнителя) администратор информационной безопасности обязан сменить пароль и сообщить его сотруднику (исполнителю).

4. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в 6 месяцев.

5. Внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться администратором информационной безопасности немедленно после окончания последнего сеанса работы данного пользователя с системой на основании письменного указания председателя Кооператива.

6. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и другие обстоятельства) администратора информационной безопасности.

7. В случае компрометации\* личного пароля пользователя ИСПДн должны быть немедленно предприняты меры в соответствии с п.5 или п.6 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

8. Порядок хранения пароля:

- запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;
- запрещается оставлять без присмотра рабочее место с незаблокированным монитором;

---

\* под компрометацией понимается утеря, передача другому лицу пароля.

– запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

– хранение пользователем своего пароля на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у администратора информационной безопасности или руководителя подразделения.

9. Контроль за действиями пользователей системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на администратора информационной безопасности.