

ИНСТРУКЦИЯ
по организации парольной защиты в информационных системах
предназначенных для обработки персональных данных в
Управлении Роспотребнадзора по ЕАО

г. Биробиджан

1. Общие положения

1.1. Настоящая инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационной системе персональных данных (далее ИСПДн) Управления Роспотребнадзора по ЕАО (далее – Управление), а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

1.2. Требования настоящей инструкции являются обязательными для исполнения всеми сотрудниками Управления.

1.3. Настоящая инструкция доводится каждому сотруднику Управления под роспись.

1.4. Контроль за выполнением требований настоящей инструкции в Управлении возлагается на администратора безопасности.

1.5. Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам защиты информации и не исключает обязательного выполнения их требований.

2. Организация парольной защиты

2.1. Парольная защита применяется для решения следующих задач:

- Обеспечение защиты информационных ресурсов от непреднамеренного воздействия, несанкционированного воздействия, разглашения, утечки, а также хищения, утраты, уничтожения, искажения или подделки за счет специальных воздействий.
- Предотвращение внедрения в автоматизированные подсистемы программ-вирусов, программных закладок.
- Защита информации ограниченного распространения.

2.2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на администратора безопасности информации.

3. Требования предъявляемые к паролю

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

- пароль сотрудником выбирается самостоятельно;
- пароль сотрудник вводит собственноручно;
- длина пароля должна быть не менее 6 символов;
- пароль должен знать только его владелец;

- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, \$, &, *, % и т.п.);
- 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 не менее чем в 4 позициях;
- личный пароль пользователь не имеет права сообщать никому.

3.2. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в месяц.

3.3. В случае компрометации личного пароля пользователя ИСПДн должна быть немедленно произведена внеплановая смена пароля в присутствии администратора безопасности.

3.4. Хранение сотрудником значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе, ответственного за информационную безопасность или начальника отдела в опечатанном личной печатью пенале (возможно вместе с персональными идентификаторами).

3.5. Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на ответственных за информационную безопасность (руководителей подразделений), периодический контроль — возлагается на администратора безопасности информации.

4. Ответственность

4.1. Пароль является служебной тайной, и каждый сотрудник несет ответственность за сохранность в тайне собственного пароля в соответствии с действующим законодательством.