«Утверждаю»
Главный врач КГП на ПХВ
«Областной онкологический диспансер»
_____ Абдримов Е.Г.

ИНСТРУКЦИЯ О ПАРОЛЬНОЙ ЗАЩИТЕ

1. Общие положения

1. Настоящая Инструкция о парольной защите регламентирует организационно-техническое обеспечение процессов генерации, использования, смены и прекращения действия личных паролей пользователей ПК и администраторов информационных систем (ИС), удаления учетных записей.

2. В целях идентификации, аутентификации и соблюдения принципа персональной ответственности за свои действия, администраторам информационных систем, пользователю должны быть присвоены учетная запись с паролями.

2. Правила формирования личного пароля

1. Личные пароли должны выбираться пользователями и администраторами ИС самостоятельно с учетом следующих требований:

1) длина пароля должна быть не менее 8 символов;

2) запрещается при авторизации пользователя использовать только логин без пароля;

3) пароль не должен включать в себя легко вычисляемые сочетания символов (имена и даты рождения своей личности и своих родственников, номера автомобилей, телефонов), которые можно угадать, основываясь на информации о пользователе, а также стандартное расположение букв на клавиатуре (zyxwvuts, 123, 123321, qwerty);

4) при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;

5) пользователь не имеет права разглашать свои личный пароль.

3. Ввод пароля

1. Во время ввода паролей, необходимо исключить возможность распознания его посторонними лицами или компрометации пароля посредством технических средств.

4. Порядок смены паролей

1. В ИС должна быть установлена принудительная смена пароля раз в месяц, вместе с этим пользователь, администратор должен иметь возможность смены пароля в любое время.
2. Сотрудник Техподдержки определяет политику смены пароля, предусматривающую срок действия пароля не более одного месяца, выдачу предупреждающего сообщения о необходимости сменить пароль и блокировку доступа к информационным ресурсам по истечению срока действия пароля.

5. Хранение пароля

3. Владельцам паролей запрещается:

1) сообщать другим пользователям личный пароль и регистрировать их в системе под своей учетной записью и паролем;

2) записывать пароли в электронной записной книжке, файле и других носителях информации, кроме бумажных носителей, при этом бумажные носители с записями паролей должны храниться в надежном и доступном только владельцу месте.

4. Пароли пользователей с именами учетных записей и датой установки паролей должны храниться в опечатанных конвертах в сейфе у руководителей структурного подразделения.

5. В случае компрометации пароля сотрудник Техподдержки, должен:

1) немедленно сменить свой пароль;

2) блокировать доступ пользователям, подключенным к ресурсам этой ИС, до смены ими своих паролей;

3) известить отдел по контролю за действиями пользователей.

6. В случае компрометации личного пароля, пользователь должен немедленно произвести внеплановую смену пароля и известить отдел по контролю за действиями пользователей.

7. При возникновении производственной необходимости в срочном доступе к данным персонального компьютера временно отсутствующего пользователя разрешается:

1) непосредственному руководителю или другому сотруднику по указанию непосредственного руководителя, вскрыть конверт с паролем и использовать компьютер;

2) произвести смену пароля пользователя его непосредственным руководителем.

При этом должен быть составлен акт о вскрытии конверта с паролем и о его повторном опечатывании с новым паролем.

Ответственность за неразглашение полученного пароля и действия, произведенные на персональном компьютере, возлагается на лицо, получившее пароль после такого случая. По прибытию, временно

отсутствующий пользователь обязан сменить пароль при первом входе в систему.

8. Учетная запись пользователя, ушедшего в длительный отпуск (более 60 дней), должна блокироваться сотрудником Техподдержки с момента получения письменного уведомления от отдела кадровой работы.

9. Удаление учетных записей пользователей, уволенных, переведенных в другое структурное подразделение, филиал, региональный центр должно производиться сотрудником службы технической поддержки немедленно с момента получения письменного уведомления из кадровой службы.

В течение 24 часов после увольнения, перевода работника в другое структурное подразделение, филиал, отдел кадровой работы должны известить Техподдержку о состоявшемся приказе.

10. Аутентификация некоторых пользователей может быть обеспечена с использованием специальных защитных аппаратно-программных средств.

6. Ответственность при организации парольной защиты

11. За разглашение парольной информации, которая представляет конфиденциальные сведения, сотрудник, привлекается к дисциплинарной ответственности согласно трудовому законодательству.