Бюджетное учреждение Республики Калмыкия
«Республиканский госпиталь ветеранов войн»

«УТВЕРЖДАЮ»
Начальник Бюджетного учреждения
Республики Калмыкия
«Республиканский госпиталь
ветеранов войн»

_____ **Л.В.Санджиева**

ПОЛОЖЕНИЕ
О ПОЛИТИКЕ ПАРОЛЬНОЙ ЗАЩИТЫ
В БЮДЖЕТНОМ УЧРЕЖДЕНИИ РЕСПУБЛИКИ КАЛМЫКИЯ
«РЕСПУБЛИКАНСКИЙ ГОСПИТАЛЬ ВЕТЕРАНОВ ВОЙН»

2012 год

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение разработано для исключения несанкционированного доступа к информационным ресурсам в целях исключения утечки конфиденциальной информации, а также несанкционированной модификации или уничтожения данных.

1.2. Аутентификация легальных субъектов доступа осуществляется с помощью парольной защиты, персонального кода доступа, электронных ключей и других программно-технических средств разграничения доступа пользователей. Способ аутентификации легальных пользователей определяется в соответствии с уровнем конфиденциальности информации. Уровень конфиденциальности данных определяется владельцем информационного ресурса по согласованию со службой безопасности.

1.3. Активное сетевое оборудование (маршрутизаторы и сетевые принтеры) не должно допускать возможности несанкционированной переконфигурации, в связи с чем, каждое активное сетевое устройство должно быть защищено уникальным паролем.

1.4. Операционные системы серверов, компьютерной сети должны настраиваться таким образом, чтобы блокировать вход в сеть (на 5-15 минут) после троекратной ошибки в наборе пароля.

1.5. Если позволяют возможности операционной системы необходимо запретить выбор пользователем простых паролей средствами операционной системы.

2. ПОРЯДОК ЗАВЕДЕНИЯ И РЕГИСТРАЦИИ СРЕДСТВ РАЗГРАНИЧЕНИЯ ПОЛЬЗОВАТЕЛЕЙ

2.1. При введении нового пользователя администратор информационного ресурса должен назначить для него однократный пароль, персональный код либо другую уникальную информацию для доступа к информационным ресурсам компьютерной сети.

2.2. Пользователь обязан заменить однократный пароль – личным при первом же подключении к информационному ресурсу компьютерной сети.

2.3. Пользователь обязан хранить в тайне пароль, код и другие средства доступа к информационным ресурсам.

3. ПЕРИОД ДЕЙСТВИЯ ПАРОЛЕЙ И КОДОВ ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ

3.1. Периодичность смены пароля задается администратором информационного ресурса централизованно, для всех пользователей.

3.2. Период действия паролей для сетевых компьютеров не должен превышать 3 месяцев, для не сетевых компьютеров – 6 месяцев.

3.3. При сообщении компьютерной системы об окончании срока действия личного пароля пользователь обязан заменить его на новый, ранее не применявшийся.

3.4. Период действия паролей для входа в АРМ автоматизированной системы не должен превышать 3 месяцев.

3.5. Персональные коды, электронные ключи и другие средства разграничения доступа меняются по требованию пользователя не реже установленного периода.

4. КОНФИДЕНЦИАЛЬНОСТЬ ПАРОЛЕЙ И КОДОВ ДОСТУПА.

4.1. Информация о паролях пользователей является конфиденциальной информацией.

4.2. Операционные системы, серверов и рабочих станций должны быть настроены таким образом, чтобы исключить возможность ознакомления пользователей и администраторов с действующими и истекшими паролями.

4.3. Автоматизированные информационные системы должны быть настроены таким образом, чтобы исключить возможность ознакомления пользователей и администраторов с действующими и истекшими паролями.

4.4. Информация о персональных кодах, электронных ключах и других средств доступа пользователей к информационному ресурсу является конфиденциальной информацией и разглашению не подлежит, должна содержать защиту от доступа посторонних лиц

5. ПРИНЦИПЫ ВЫБОРА И ФОРМИРОВАНИЯ ЛИЧНЫХ ПАРОЛЕЙ

5.1. В качестве парольной информации следует выбирать последовательность букв верхнего и нижнего регистра, цифр и служебных символов длиной не менее восьми знаков.

5.2. Категорически запрещается использование в качестве пароля легко угадываемых последовательностей символов типа: названия учетной записи, номеров телефонов, имен своих и родственников, последовательно расположенные на стандартной клавиатуре символы, табельный номер и т.п. Запрещается также использование в качестве паролей слов распространенных мировых языков, независимо от раскладки клавиатуры, в которой оно набирается (например, слово МАШИНА – VFIBYF).

5.3. В пароле, кроме буквенных последовательностей, обязательно должны присутствовать цифры и специальные символы.

5.4. Если позволяют возможности системы аутентификации рекомендуется наряду с английскими буквами использовать буквы русского алфавита (с переключением набора символов на клавиатуре).

5.5. Рекомендуется в виде пароля выбирать последовательности типа “X0Posh#1”, “1рыБ@lkA” или “Def*en$6”

5.6. При смене пароля пользователям запрещается использовать ранее использованные пароли.

5.7. Выбор одноразовых паролей осуществляется по тем же требованиям.

5.8. Длина пароля администратора информационного ресурса должна быть не менее 11 символов. Пароль не должен содержать никакой логики. Например “k$iu^sd26Fx”. Глубина истории пароля не менее 20.

6. ПРАВИЛА РАБОТЫ И ОБЯЗАННОСТИ СОТРУДНИКОВ ПО ИСПОЛЬЗОВАНИЮ И СОХРАНЕНИЮ В ТАЙНЕ ЛИЧНОГО ПАРОЛЯ

6.1. Разрешается записывать названия учетных записей и пароли пользователя на бумагу (дискету). В этом случае они в опечатанном виде (в конверте), исключающем случайное ознакомление, передается в сейф начальнику подразделения (отдела). Пароли могут быть выданы только владельцу. В случае нарушения опечатки на конверте или его утери, пароли считается скомпрометированными и подлежит немедленной смене.

6.2. Если пользователь уверен в правильности ввода названия учетной записи и пароля, но ему не удается войти в систему, пользователь обязан незамедлительно сообщить об этом администратору информационного ресурса для получения нового одноразового пароля.

6.3. Если пользователь заметит несанкционированное появление, изменение или удаление информации, он должен немедленно изменить свой пароль и сообщить об обнаруженных изменениях начальнику отдела, администратору информационного ресурса и администратору информационной безопасности.

6.4. Набор личного пароля следует проводить, в отсутствии лиц, которые потенциально могут увидеть процесс набора.

6.5. При оставлении рабочего места необходимо завершить открытую пользовательскую сессию либо использовать функцию «временной блокировки» рабочей станции.

6.6. Для предотвращения случайного оставления рабочего места с открытой пользовательской сессией рекомендуется использовать ScreenSaver с автоматической блокировкой, включающийся автоматически, если компьютер не используется в течение определенного времени (5-15 минут).

6.7. Запрещается:

6.7.1. Передача личного пароля сослуживцам или руководителям подразделения;

6.7.2. Запись личного пароля доступа на материальные носители (напр. бумагу, дискеты) в открытом виде;

6.7.3. Вход в компьютерную сеть и информационную систему с использованием чужих идентификаторов и паролей доступа;

6.7.4. Оставлять без присмотра рабочее место с открытой пользовательской сессией.

6.8. В случае подозрения о компрометации пароля, сотрудники обязаны произвести экстренную замену личного пароля и незамедлительно поставить об этом в известность администратора информационной безопасности для исключения возможности утечки информации.

6.9. Любые действия сотрудников и посторонних лиц нарушающие требования настоящего Положения, категорируемые как значимые нарушения и нарушения, имеющие признаки компьютерного преступления, должны анализироваться через процедуру служебного расследования.