Министерство по физической культуре и спорту Челябинской области
ОБЛАСТНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ «РЕГИОНАЛЬНЫЙ ЦЕНТР СПОРТИВНОЙ ПОДГОТОВКИ ПО ДЗЮДО ЧЕЛЯБИНСКОЙ ОБЛАСТИ ИМЕНИ ЗАСЛУЖЕННОГО ТРЕНЕРА РОССИИ А.Е.МИЛЛЕРА»
(ОБУ «РЦСП по дзюдо Челябинской области имени А.Е. Миллера»)

Приложение 7

УТВЕРЖДЕНА
приказом директора
ОБУ «РЦСП по дзюдо
Челябинской области
имени А.Е. Миллера»

от 30.03.2023 № 125-ОД

г.Челябинск

ИНСТРУКЦИЯ
по организации парольной защиты областного бюджетного учреждения «Региональный центр спортивной подготовки по дзюдо Челябинской области имени Заслуженного тренера России А.Е.Миллера»

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Данная инструкция регламентирует процессы генерации, смены и прекращения действия паролей (удаления учётных записей пользователей) в информационных системах (далее – ИС) областного бюджетного учреждения «Региональный центр спортивной подготовки по дзюдо Челябинской области имени Заслуженного тренера России А.Е.Миллера» (далее - ОБУ «РЦСП по дзюдо Челябинской области имени А.Е.Миллера»), а также контроль над действиями пользователей при работе с паролями.

1.2. Осуществление процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИС и контроль за действиями пользователей при работе с паролями возлагается на ответственного за обеспечение безопасности персональных данных в информационных системах.

II. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. **Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»).

2.2. **Информационная система (ИС)** – система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные

ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию.

2.3. **Пароль** – секретная комбинация цифр, знаков, слов, или осмысленное предложение, служащие для защиты информации от несанкционированного доступа к информационным ресурсам.

2.4. **Пользователь** – работник, участвующий в рамках своих функциональных обязанностей в процессах обработки персональных данных.

2.5. **Компрометация пароля** – раскрытие, обнаружение или утеря пароля.

III. ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

3.1. Правила формирования паролей:

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

3.1.1.1. длина пароля должна быть не менее 6 символов;

3.1.1.2. в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

3.1.1.3. пароль не должен включать в себя имя пользователя, легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, абвгд и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе.

3.1.1.4. при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6-ти позициях;

3.1.2. Пользователям допускается использовать пароли, составленные из первых букв слов запоминающихся высказываний в разном регистре, смешанные в произвольном порядке со специальными символами (например, Кожзгсф7!).

3.1.3. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на ответственного за обеспечение безопасности персональных данных в информационных системах.

3.2. Порядок смены личных паролей:

3.2.1. Смена паролей должна проводиться регулярно, не реже одного раза в 3 месяца.

3.2.2. В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т.п.) должно производиться немедленное удаление его учётной записи сразу после окончания последнего сеанса работы данного пользователя с системой.

3.2.3. Срочная (внеплановая) полная смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) ответственных за обеспечение безопасности персональных данных в информационных системах, администраторов информационной системы и других работников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

3.2.4. Ответственный за обеспечение безопасности персональных данных в информационных системах ведёт Журнал учёта работ в информационных системах, в котором он отмечает факт смены паролей пользователей.

3.2.4.1. Временный пароль, заданный ответственным за обеспечение безопасности персональных данных в информационных системах при регистрации нового пользователя, должен действовать в течение ограниченного срока времени. Пользователь должен изменить временный пароль при первом входе в систему.

3.3. В ИС должна обеспечиваться защита аутентификационной информации в процессе ее ввода от возможного использования лицами, не имеющими на это полномочий. Защита обеспечивается отображением вводимых символов условными знаками «*», «•» или иными знаками, вместо действительной информации.

3.4. Действия в случае утери и компрометации пароля:

3.4.1. В случае утери или компрометации (разглашения, утраты) или подозрения в компрометации пароля пользователя должна быть немедленно проведена внеплановая процедура смены пароля.

IV. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ ИС

4.1. Правила формирования паролей:

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

4.1.1.1. длина пароля должна быть не менее 6 символов;

4.1.1.2. в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

4.1.1.3. пароль не должен включать в себя имя пользователя, легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, абвгд и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе;

4.1.1.4. при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6-ти позициях.

4.1.2. Работникам допускается использовать пароли, составленные из первых букв слов запоминающихся высказываний в разном регистре, смешанные в произвольном порядке со специальными символами (например, Кожзгсф7!).

4.1.3. Для обеспечения возможности использования имён и паролей некоторых работников в их отсутствие (например, в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п.), работники обязаны сразу же после установки своих паролей передавать их на хранение вместе с именами своих учетных записей ответственному за обеспечение безопасности персональных данных в информационных системах в запечатанном конверте или опечатанном пенале.

4.2. Порядок ввода пароля:

4.2.1. При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его подсматривания посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев в прямой видимости или в отраженном свете) и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т.п.).

4.3. Порядок смены личных паролей:

4.3.1. Смена паролей должна проводиться регулярно, не реже одного раза в 3 месяца, самостоятельно каждым пользователем.

4.3.2. Временный пароль, заданный ответственным за обеспечение безопасности персональных данных в информационных системах при регистрации нового пользователя, должен действовать в течение ограниченного срока времени. Пользователь должен изменить временный пароль при первом входе в систему.

4.4. Хранение пароля:

4.4.1. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке, мобильном телефоне и любых других предметах и носителях информации.

4.4.2. Запрещается сообщать свой пароль полностью или частично другим пользователям, запрещается спрашивать или подсматривать пароль других пользователей.

4.4.3. Запрещается регистрировать других пользователей в ИС со своим личным паролем, запрещается входить в ИС под учётной записью и паролем другого пользователя.

4.5. Действия в случае утери и компрометации пароля:

4.5.1. В случае утери или компрометации (разглашения, утраты) или подозрения в компрометации пароля пользователь должен немедленно обратиться к ответственному за обеспечение безопасности персональных данных в информационных системах с целью смены личного пароля.

V. ОТВЕТСТВЕННОСТЬ

5.1. Работники несут персональную ответственность за соблюдение требований настоящей Инструкции, за качество проводимых ими работ по обеспечению безопасности информации и за все действия, совершенные от имени их учётных записей в ИС, если с их стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.

5.2. Работники при нарушении норм, регулирующих получение, обработку и защиту информации, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

5.3. Разглашение информации (передача их посторонним лицам, в том числе другим работникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных локальными нормативно-правовыми актами (приказами, распоряжениями) ОБУ «РЦСП по дзюдо Челябинской области имени А.Е.Миллера», влечет наложение на работника, имеющего доступ к защищаемой информации, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Работник ОБУ «РЦСП по дзюдо Челябинской области имени А.Е.Миллера», имеющий доступ к информации и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба ОБУ «РЦСП по дзюдо Челябинской области имени А.Е.Миллера» (в соответствии с п.7 ст. 243 Трудового кодекса РФ).

5.3.1. В отдельных случаях, при разглашении персональных данных, работник, совершивший указанный проступок, несет ответственность в соответствии со ст. 13.14 Кодекса об административных правонарушениях РФ.

5.4. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст. 137 Уголовного кодекса РФ.