Приложение 1
к приказу директора филиала
от 14.10.2022 №01-24/217

Инструкция парольной защиты информационных ресурсов филиала «Колледж современных технологий в машиностроении и автосервисе» учреждения образования «Республиканский институт профессионального образования»

1. Аннотация

Настоящая Инструкция разработана для использования работниками филиала «Колледж современных технологий в машиностроении и автосервисе» учреждения образования «Республиканский институт профессионального образования» (далее - филиал КСТМиА УО РИПО) с целью усиления парольной защиты в информационных системах персональных данных филиала КСТМиА УО РИПО, минимизации рисков несанкционированного доступа и снижению финансовых рисков, связанных с парольной политикой. Целевой пользователь документа – работники филиала КСТМиА УО РИПО.

2. Требования

Все правила в области парольной политики, применяемые в филиале КСТМиА УО РИПО, в случае их регламентации, при генерации (создании) новых парольных фраз должны быть оптимизированы с учетом следующих требований:

1. Пароли определяются работниками самостоятельно с учетом следующих требований:

длина пароля должна быть не менее 8 символов;

в числе символов обязательно должны присутствовать минимум одна прописная буква латинскими, одна строчная буква латинская, цифра и специальный символ ($, @, #, %, & и т.п.);

пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов, даты рождения и т.п.);

пароль не должен быть часто употребляемым словом;

пароль не должен содержать ФИО, дату рождения, номер телефона, номер, автомобиля, название организации.

2. Запрещается:

оставлять рабочий компьютер без блокировки экрана монитора;

передача паролей другим работникам;

передача паролей пользователя при помощи почтовых сообщений либо иным другим открытым способом через Интернет;

оставлять пароль, записанный на бумажном носителе, в доступном для посторонних лиц месте (в том числе на рабочем столе, экране монитора);

вводить пароль от учетной записи при посторонних лицах.

3. Плановая смена паролей должна проводится регулярно, не реже 1 раз в 90 дней.

4. Внеплановая смена паролей производится в случаях:

смены рабочего места;

обнаружения признаков нарушения системы защиты персональных данных.

3. Требования к передаче парольно-ключевой информации

В случае незапланированного отсутствия работника на рабочем месте передача парольно-ключевой информации возможна в случае служебной (оперативной) необходимости. Работник имеет право передать свои учетные данные непосредственному руководителю (или лицу его замещающему) для решения оперативных задач в целях поддержания непрерывности рабочего процесса. Передача парольной информации должна осуществляться способом, отвечающим требованиям конфиденциальности, с учетом фактической ситуации внепланового отсутствия.

По возвращению к должностным обязанностям работник обязан изменить пароль своей учетной записи. Ответственность за полученную парольно-ключевую информацию и ресурсы ею защищаемые возлагается на лицо, получившее такой доступ.

В непредусмотренных настоящими требованиями случаях (например, невозможности установления связи с работником) допускается следующий механизм получения парольно-ключевой информации: работник, которому необходимо получить доступ к автоматизированному рабочему месту, по согласованию с руководителем структурного подразделения (или лицом его замещающим) обращается к ведущему инженеру-программисту в рабочем порядке. Ведущему инженеру-программисту, установив возможность предоставления доступа, предоставляет доступ к автоматизированному рабочему месту посредством использования учетной записи Администратора.

Передача парольно-ключевой информации (логина и/или пароля) третьим лицам запрещена.

Блокировка экрана должна производиться через минуту бездействия пользователя. В случаи необходимости покинуть рабочее место, требуется заблокировать экран сочетанием клавиш win+L.

4. Рекомендации

В целях усиления уровня защищенности при применении правил парольной защиты пользователям следует придерживаться следующих рекомендаций:

при вводе пароля, пользователю необходимо исключить 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.);

в случае прекращения полномочий пользователя (увольнение, либо переход на другую должность) производится немедленное удаление пароля сразу после окончания его последнего дня работы;

срочная (внеплановая) полная смена паролей должна производиться в случае прекращения полномочий (увольнение или переход на другую работу) администраторов информационной системы и других работников, которым по функциональным обязанностям были предоставлены полномочия по управлению системой парольной защиты;

не используйте один и тот же пароль для доступа к учётным записям филиала КСТМиА УО РИПО и к другим ресурсам (например, доступ в интернет из дома, системам электронной коммерции и т.д.). По возможности не используйте один и тот же пароль для доступа к различным ресурсам внутри филиала КСТМиА УО РИПО;

не использовать ранее использованные пароли;

не сообщайте никому свой пароль по телефону;

не отправляйте свой пароль по электронной почте;

не говорите о своём пароле рядом с посторонними.

не упоминайте о содержимом пароля (например, «мой день рождения»);

не указывайте свой пароль в анкетах или опросниках;

не храните пароль в файле на компьютере, включая переносной, без шифрования;

не используйте функцию «Запомнить пароль», например, в таких приложениях как Google Chrome и т.д.;

если кто-либо требует сообщить ваш пароль, сошлитесь на этот документ или попросите позвонить ведущему инженеру-программисту;

если вы считаете, что учётная запись или пароль скомпрометированы, сообщите об этом и ведущему инженеру-программисту, смените все пароли.

5. Ответственность

Работники филиала КСТМиА УО РИПО несут ответственность за сохранность парольной информации и соблюдение положений настоящей инструкции.

За невыполнение требований по защите персональных данных физические лица могут быть привлечены к дисциплинарной и административной ответственности, в случае, если - не обеспечена сохранность данных (абз. 6 п. 3 ст. 17 Закона о защите персональных данных);

Умышленное незаконное распространение персональных данных физлиц карается штрафом в размере до 200 БВ (ч. 3 ст. 23.7 КоАП). Под распространением понимают действия, направленные на ознакомление с персональными данными неопределенного круга лиц (абз. 11 ст. 1 Закона о защите персональных данных). В том числе передача пароля третьим лицам.

К **уголовной ответственности** могут привлечь только физлицо (ст. 27, 28 УК).

Уголовная ответственность предусмотрена за:

умышленные незаконные сбор, предоставление персональных данных другого лица без его согласия, повлекшие причинение существенного вреда правам, свободам и законным интересам гражданина. Наказание - общественные работы, или штраф, или арест, или ограничение или лишение свободы на срок до двух лет (ч. 1 ст. 203-1 УК);

несоблюдение мер обеспечения защиты персональных данных лицом, осуществляющим их обработку, повлекшее по неосторожности их распространение и причинение тяжких последствий. Наказание - штраф, или лишение права занимать определенные должности или заниматься определенной деятельностью, или исправительные работы на срок до одного года, или арест, или ограничение свободы на срок до двух лет, или лишение свободы на срок до одного года (ст. 203-2 УК).

Владельцы личных паролей должны быть ознакомлены под подпись с данной инструкцией и предупреждены об ответственности за разглашение парольной информации.

Ведущий инженер-программист организует периодический контроль на ЭВМ сотрудников за правильностью обращения с личными паролями, соблюдением порядка их смены и хранения.

Руководители структурных подразделений (заместители директора, начальники отделов) организует периодический контроль на рабочих местах пользователей за правильностью обращения с личными паролями, соблюдением порядка их смены и хранения.

В случае выявления нарушений установленного порядка работы с личными паролями или нарушения функционирования автоматизированного рабочего места пользователя требовать прекращения обработки информации, как для отдельных пользователей, так и в подсистеме в целом до выяснения их причин и замены личного пароля пользователя (пользователей).

Юрисконсульт
_____ О.Г.Леончикова
14.10.2022

Ведущий инженер-программист
_____ П.В.Михайлов
14.10.2022