Министерство образования и молодежной политики Свердловской области

государственное автономное профессиональное образовательное учреждение Свердловской области «Ирбитский мотоциклетный техникум» (ГАПОУ СО «ИМТ»)

Директор ГАПОУ СО «ИМТ»

_____ С.А. Катцина

«30» декабря 2019 г.

МП

ИНСТРУКЦИЯ

по организации парольной защиты персональных данных в информационных системах персональных данных

государственного автономного профессионального образовательного учреждения Свердловской области «Ирбитский мотоциклетный техникум»

2019 год

г. Ирбит

Номер документа	СП-03-2019-№ 3.3-05
Документ вводится	Взамен Инструкции по организации парольной защиты персональных данных в информационных системах персональных данных ГАПОУ СО «ИМТ», 2015

РАССМОТРЕНО
Советом Автономного учреждения
Протокол № 10
от «26» декабря 2019 г.

Утверждено и введено в действие
приказом директора ГАПОУ СО «ИМТ»
№392-од от «30» декабря 2019 г.

Инструкция по организации парольной защиты персональных данных в информационных системах персональных данных государственного автономного профессионального образовательного учреждения Свердловской области «Ирбитский мотоциклетный техникум», 2019

Инструкция по организации парольной защиты персональных данных в информационных системах персональных данных государственного автономного профессионального образовательного учреждения Свердловской области «Ирбитский мотоциклетный техникум» регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах персональных данных ГАПОУ СО «ИМТ», а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

ИНСТРУКЦИЯ
по организации парольной защиты персональных данных в информационных системах персональных данных государственного автономного профессионального образовательного учреждения Свердловской области «Ирбитский мотоциклетный техникум»

СОДЕРЖАНИЕ

ИНСТРУКЦИЯ
по организации парольной защиты персональных данных в информационных системах персональных данных государственного автономного профессионального образовательного учреждения Свердловской области «Ирбитский мотоциклетный техникум»

1.ОБЩИЕ ПОЛОЖЕНИЯ

1. Инструкция по организации парольной защиты персональных данных (далее – ПДн) в информационных системах персональных данных (далее – ИСПДн) государственного автономного профессионального образовательного учреждения Свердловской области «Ирбитский мотоциклетный техникум» (далее – настоящая Инструкция) является локальным нормативным актом государственного автономного профессионального образовательного учреждения Свердловской области «Ирбитский мотоциклетный техникум» (далее – Автономного учреждение), регламентирующим деятельность Автономного учреждения по обеспечению безопасности персональных данных работников организации, участников образовательного процесса.

2. Настоящая инструкция разработана в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», другими нормативными правовыми актами по обеспечению безопасности персональных данных и регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в ИСПДн Автономного учреждения, а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

3. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн Автономного учреждения и контроль за действиями исполнителей и обслуживающего персонала при работе с паролями возлагается на системного администратора Автономного учреждения.

2. ПРАВИЛА ФОРМИРОВАНИЯ ПАРОЛЯ

4. Персональные пароли генерируются и распределяются либо централизованно (системным администратором Автономного учреждения), либо выбираются пользователями ИСПДн самостоятельно с учетом следующих требований:

1) пароль должен состоять не менее чем из шести символов;

2) в пароле желательно присутствие буквы из верхнего и нижнего регистров, цифры и специальные символы (@, #, $, &, *, % и т. п.);

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

4) при смене пароля новый пароль должен отличаться от старого не менее чем в двух позициях;

5) запрещается использовать в качестве пароля «пустой» пароль, имя входа в систему, простые пароли типа «123», «111» и им подобные, а так же имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов

и другие пароли, которые можно угадать, основываясь на информации о пользователе;

6) личный пароль пользователь не имеет права никому сообщать.

5. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на системного администратора Автономного учреждения.

6. При наличии в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п. технологической необходимости использования имен и паролей некоторых пользователей в их отсутствие, такие пользователи обязаны сразу же после смены своих паролей их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте передавать на хранение администратору безопасности информации или руководителю своего подразделения. Опечатанные конверты с паролями пользователей должны храниться в сейфе. Для их опечатывания рекомендуется использовать печать отдела кадров.

3. ВВОД ПАРОЛЯ

7. 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 видеокамерам и т.п.).

4. ПОРЯДОК СМЕНЫ ПАРОЛЯ

8. Полная плановая смена паролей должна проводится системным администратором Автономного учреждения или пользователем ИСПДн регулярно, не реже одного раза в 2 месяца.

9. В случае прекращения полномочий пользователя (увольнение, либо переход на другую работу), системный администратор должен немедленно удалить его учетную запись сразу после окончания последнего сеанса работы данного пользователя с системой.

10. Срочная (внеплановая) полная смена паролей должна производится в случае прекращения полномочий (увольнение или переход на другую работу) системного администратора Автономного учреждения.

11. Смена пароля производится самостоятельно каждым пользователем в соответствии с п. 2.3 настоящей Инструкции и/или в соответствии с указанием в системном баннере-предупреждении (при наличии технической возможности).

12. Временный пароль, заданный системным администратором при регистрации нового пользователя, следует изменить при первом входе в систему.

13. Системный администратор ведет "Журнал принудительной смены личных паролей", в котором отмечает причины внеплановой смены паролей пользователей.

5. ХРАНЕНИЕ ПАРОЛЯ

14. Хранение пользователем своего пароля на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе либо в сейфе у системного администратора или руководителя подразделения в опечатанном пенале.

15. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.

16. Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

6. ДЕЙСТВИЯ В СЛУЧАЕ УТЕРИ И КОМПРОМЕНАЦИИ ПАРОЛЯ

17. В случае утери или компрометации пароля пользователя должны быть немедленно предприняты меры в соответствии с п. 10 или 11. настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

7. ОТВЕТСТВЕННОСТЬ ПРИ ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ

18. Владельцы паролей должны быть ознакомлены под подпись с настоящей Инструкцией и предупреждены об ответственности (Приложение № 1 к настоящей Инструкции) за использование паролей, не соответствующих требованиям настоящей Инструкции, а также за разглашение информации о пароле и за использование, хранение и потерю присвоенных идентификатора и пароля.

19. В случае утечки информации о зарегистрированном пользователе необходимо НЕМЕДЛЕННО УДАЛИТЬ данные об этом пользователе и ЗАРЕГИСТРИРОВАТЬ ЗАНОВО его с новым идентификатором.

20. Ответственность за организацию парольной защиты в структурных подразделениях техникума возлагается на системного администратора.

21. Периодический контроль за соблюдением требований настоящей Инструкции возлагается на системного администратора Автономного учреждения.

22. Работники Автономного учреждения и лица, имеющие отношение к обработке ПДн в ИСПДн должны быть ознакомлены под подпись с настоящей Инструкцией.

8. ПРОЦЕДУРА ВНЕДРЕНИЯ И ОБЕСПЕЧЕНИЯ НАСТОЯЩЕЙ ИНСТРУКЦИИ

23. Настоящая Инструкция вводится в действие приказом директора Автономного учреждения.

24. Настоящая Инструкция принимается к действию лицами, допущенными к ПДн при их обработке в ИСПДн под подпись, с даты введения инструкции.

25. Системный администратор Автономного учреждения ведет Журнал выдачи паролей и учета пользователей (в случае централизованного распределения персональных паролей).

Журнал (Приложение № 2 к настоящей Инструкции) хранится у системного администратора Автономного учреждения.

26. Настоящая Инструкция принимается на неопределенный срок. Изменения и дополнения в настоящую Инструкцию вносятся и рассматриваются в составе новой редакции на Совете Автономного учреждения и утверждаются приказом директора Автономного учреждения.

Приложение № 1

ПЕРЕЧЕНЬ СТАТЕЙ
законодательства Российской Федерации, предусматривающих ответственность за нарушение норм по обработке и защите сведений, полученных при осуществлении доступа к охраняемой законом компьютерной информации

КОДЕКС ОБ АДМИНИСТРАТИВНЫХ ПРАВОНАРУШЕНИЯХ

Статья 13.14. Разглашение информации с ограниченным доступом

Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, за исключением случаев, предусмотренных частью 1 статьи 14.33 настоящего Кодекса, - влечет наложение административного штрафа на граждан в размере от пятисот до одной тысячи рублей; на должностных лиц - от четырех тысяч до пяти тысяч рублей.

УГОЛОВНЫЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ

Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, -

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности, - наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, - наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, - наказываются лишением свободы на срок до семи лет.

Примечания. 1. Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

2. Крупным ущербом в статьях настоящей главы признается ущерб, сумма которого превышает один миллион рублей.

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ

1. Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, -наказываются ограничением свободы на срок до четырех лет, либо

принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

2. Деяния, предусмотренные частью первой настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности, - наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере от ста тысяч до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, - наказываются лишением свободы на срок до семи лет.

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

1. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб, - наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. Деяние, предусмотренное частью первой настоящей статьи, если оно повлекло тяжкие последствия или создало угрозу их наступления, - наказывается принудительными работами на срок до пяти лет либо лишением свободы на тот же срок.

ТРУДОВОЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ

Статья 57. Содержание трудового договора

«…В трудовом договоре могут предусматриваться дополнительные условия, не ухудшающие положение работника по сравнению с установленным трудовым законодательством и иными нормативными правовыми актами, содержащими нормы трудового права, коллективным договором, соглашениями, локальными нормативными актами, в частности:
- о неразглашении охраняемой законом тайны (государственной, служебной, коммерческой и иной);
- об уточнении применительно к условиям работы данного работника прав и обязанностей работника и работодателя, установленных трудовым законодательством и иными нормативными правовыми актами, содержащими нормы трудового права…»

Статья 86. Общие требования при обработке персональных данных работника и гарантии их защиты

В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника обязаны соблюдать следующие общие требования:

1) обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

2) при определении объема и содержания обрабатываемых персональных данных работника

работодатель должен руководствоваться Конституцией Российской Федерации, настоящим Кодексом и иными федеральными законами;

3) все персональные данные работника следует получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение;

4) работодатель не имеет права получать и обрабатывать сведения о работнике, относящиеся в соответствии с законодательством Российской Федерации в области персональных данных к специальным категориям персональных данных, за исключением случаев, предусмотренных настоящим Кодексом и другими федеральными законами;

5) работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных настоящим Кодексом или иными федеральными законами;

6) при принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения;

7) защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном настоящим Кодексом и иными федеральными законами;

8) работники и их представители должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области;

9) работники не должны отказываться от своих прав на сохранение и защиту тайны;

10) работодатели, работники и их представители должны совместно вырабатывать меры защиты персональных данных работников.

Статья 87. Хранение и использование персональных данных работников

Порядок хранения и использования персональных данных работников устанавливается работодателем с соблюдением требований настоящего Кодекса и иных федеральных законов.

Статья 88. Передача персональных данных работника

При передаче персональных данных работника работодатель должен соблюдать следующие требования:

- не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных настоящим Кодексом или иными федеральными законами;
- не сообщать персональные данные работника в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном настоящим Кодексом и иными федеральными законами;
- осуществлять передачу персональных данных работника в пределах одной организации, у одного индивидуального предпринимателя в соответствии с локальным нормативным актом, с которым работник должен быть ознакомлен под роспись;
- разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;

- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;
- передавать персональные данные работника представителям работников в порядке, установленном настоящим Кодексом и иными федеральными законами, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

Статья 89. Права работников в целях обеспечения защиты персональных данных, хранящихся у работодателя

В целях обеспечения защиты персональных данных, хранящихся у работодателя, работники имеют право на:
- полную информацию об их персональных данных и обработке этих данных;
- свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом;
- определение своих представителей для защиты своих персональных данных;
- доступ к медицинской документации, отражающей состояние их здоровья, с помощью медицинского работника по их выбору;
- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований настоящего Кодекса или иного федерального закона. При отказе работодателя исключить или исправить персональные данные работника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;
- требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных.

Статья 90. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника

Лица, виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном настоящим Кодексом и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

Приложение № 2
Типовая форма

ЖУРНАЛ
выдачи паролей и учета пользователей (субъектов доступа) ИСПДн
ГАПОУ СО «ИМТ»

№ п/п	ФИО	Имя пользователя	Место работы и должность	Дата выдачи разрешения/ пароля	Перечень ресурсов в соответствии с разрешением	Права доступа	Дата регистрации пользователя, подпись	Изменение прав доступа	Подпись

_____ _____
ФИО, должность ответственного лица за организацию хранения и ведения журнала подпись