Приложение № 3
к приказу ГАПОУ МИК
от «___»_____20___ года №_____

УТВЕРЖДАЮ
Директор ГАПОУ МИК
_____И.В.Горшкова
«___»_____2021г.

Положение
об организации парольной защиты в
ГАПОУ МИК

I. Общие положения

1. Положение об организации парольной защиты ГАПОУ МИК (далее – Положение) регламентирует:

организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационной среде;

меры обеспечения безопасности при использовании паролей;

меры контроля за действиями пользователей и обслуживающего персонала при работе с паролями.

2. Требования настоящего Положения:

являются неотъемлемой частью комплекса мер безопасности и защиты информации в ГАПОУ МИК (далее – образовательное учреждения);

распространяются на сотрудников образовательного учреждение) ;

обязательны к применению для всех средств вычислительной техники, эксплуатируемой в образовательном учреждении) , а также информационных систем и сервисов, используемых сотрудниками образовательного учреждения).

3. Ознакомление с Положением является выражением согласия с персональной ответственностью за разглашение парольной информации лицам, не имеющим права на доступ к таким сведениям.

4. Сведения о логине и пароле в сочетании и раздельно – являются конфиденциальной информацией, на которую распространяется действие нормативных правовых актов образовательного учреждения, принятых в отношении конфиденциальной информации.

5. Термины и определения:

Автоматизированная система (АС) – совокупность программных и аппаратных средств, предназначенных для хранения, передачи и обработки информации и производства вычислений.

АРМ (автоматизированное рабочее место) – программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида АС.

Информационная безопасность (ИБ) – обеспечение защищенности информации (ее конфиденциальности, целостности, доступности) от широкого спектра угроз с целью обеспечения непрерывности работы и минимизации рисков.

Ключевой носитель – электронный носитель (дискета, флэш-накопитель, компакт-диск, токен и т.п.), на котором находится ключевая информация (ключи доступа, пароли, любая информация, позволяющая получить привилегии, права, полномочия в информационной среде).

Компрометация – утрата доверия к тому, что информация недоступна посторонним лицам.

Несанкционированный доступ (НСД) – доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа.

Принцип минимальных привилегий – принцип, согласно которому каждому субъекту системы предоставляется минимальный набор полномочий (или минимальный допуск), необходимый для выполнения вверенных задач. Применение этого принципа ограничивает ущерб, наносимый в результате случайного, ошибочного или несанкционированного использования системы.

Сотрудник – работник образовательного учреждения.

Учетная запись – информация о пользователе: имя пользователя, его пароль, права доступа к ресурсам и право выполнения определенных операций с данными в системе. Учетная запись может содержать дополнительную информацию (адрес электронной почты, телефон и т.п.).

II. Общие требования к паролям

6. Пароли доступа к информационной системе (сервису) первоначально формируются оператором данной системы (сервиса) или назначенным на данную роль сотрудником. В дальнейшем пользователь информационной системы (сервиса) должен самостоятельно изменить пароль на собственный, с учетом требований Положения, предъявляемых к паролю.

7. Запрещается использовать в качестве пароля любую информацию, относящуюся к сотруднику или месту его работы (дата или год рождения сотрудника или близких ему людей, имена детей, клички домашних животных и др.).

8. Пароли должны отвечать следующим требованиям:

длина пароля должна быть не менее 10 символов (для привилегированных учетных записей – не менее 12 символов);

при смене пароля новый пароль должен отличаться от старого не менее, чем двумя символами.

III. Безопасность локальных учетных записей на АРМ работников

9. Локальные учетные записи на АРМ сотрудников используются только при настройке операционной системы и не предназначены для повседневной работы.

10. Пользователям запрещено создание и использование учетных записей на АРМ, подключенных к компьютерной сети образовательного учреждения и входящих в состав домена либо какого-либо из его поддоменов.

11. Встроенная гостевая учетная запись должна быть заблокирована на всех АРМ в составе компьютерной сети образовательного учреждения при первоначальном конфигурировании операционной системы.

12. Встроенная административная учетная запись операционной системы на АРМ образовательного учреждения должна быть отключена администратором домена. Допускается отсутствие блокировки административной учетной записи операционной системы, если АРМ образовательного учреждения не включен в домен. В этом случае такая учетная запись должна быть защищена паролем, отвечающим требованиям п. 8 Положения.

13. Базовая система ввода-вывода (BIOS) рабочих станций на АРМ образовательного учреждения должна быть защищена паролем длиной не менее 8 символов.

IV. Безопасность учетных записей работников ГАПОУ МИК

14. Создание, изменение, удаление учетной записи сотрудника образовательного учреждения (домен, электронная почта и др.) производится после получения заявки от руководителя структурного подразделения образовательного учреждения, для сотрудника которого необходимо выполнить одно из указанных выше действий.

15. Сотрудник несет персональную ответственность за сохранение в тайне личного пароля. Запрещается сообщать пароль другим лицам, а также хранить записанный пароль в общедоступных местах.

16. Допускается раскрытие пароля работника при проведении проверочных мероприятий управлением информационной безопасности образовательного учреждения (ответственный за информационную безопасность) или при производственных работах. После данных работ работник самостоятельно производит немедленную смену «раскрытых» паролей.

17. В случае возникновении нештатных ситуаций, форс-мажорных обстоятельств, а также технологической необходимости использования имени и пароля сотрудника (в его отсутствие) допускается изменение пароля руководителем сотрудника. В таких случаях, сотрудник, чей пароль был изменен, обязан после выявления факта смены своего пароля, незамедлительно создать новый пароль.

18. Пароли учетных записей пользователей АС должны соответствовать требованиям п. 8 Положения.

19. Управление доменными учетными записями пользователей осуществляется исходя из принципа «минимальных привилегий», т.е. пользователь не должен иметь прав доступа как к локальной системе, так и к ресурсам АС больше, чем это необходимо ему для выполнения своих должностных обязанностей.

20. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в 6 месяцев. Плановая смена должна предусматривать информирование пользователя о необходимости сменить пароль и возможность смены пароля без обращения к сотруднику, обслуживающему контроллер домена или АС образовательного учреждения.

21. Внеплановая смена личного пароля или удаление учетной записи пользователя АС в случае прекращения его полномочий (увольнение, переход на работу в другое структурное подразделение образовательного учреждения и иные обстоятельства.) должна организовываться руководителем структурного подразделения образовательного учреждения, в котором он осуществляет трудовую функцию, либо вышестоящим должностным лицом незамедлительно после окончания последнего сеанса работы данного пользователя.

22. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на работу в другое структурное подразделение образовательного учреждения и иные обстоятельства) сотрудников, которым были предоставлены полномочия по управлению парольной защитой подсистем контроллера домена или АС образовательного учреждения.

23. В случае длительного (более 14 дней) отсутствия сотрудника образовательного учреждения (командировка, болезнь и т.п.) его учетная запись блокируется.

24. В случае компрометации или утраты личного пароля либо подозрения на компрометацию сотрудником образовательного учреждения незамедлительно должны быть предприняты меры по внеплановой смене личного пароля с информированием руководителя структурного подразделения образовательного учреждения в котором он осуществляет трудовую функцию, либо вышестоящего должностного лица.

25. В случае, если сотрудник образовательного учреждения забыл личный пароль (и при этом пароль не скомпрометирован и не утрачен) он обязан обратиться к администратору контроллера домена или АС образовательного учреждения с просьбой о восстановлении пароля. Администратор контроллера домена или АС обязан установить временный пароль в соответствие с требованиями п. 8 Положения. Пользователь после получения временного пароля обязан в кратчайшее время (не более 30 минут) сменить временный пароль.

26. Для предотвращения подбора паролей в контроллере домена или АС образовательного учреждения должна осуществляться блокировка учетной записи при пятикратном неправильном вводе пароля.

27. При временном оставлении рабочего места в течение рабочего дня сотрудник обязан заблокировать АРМ до интерфейса с предложением о входе в операционную систему.

28. При возникновении вопросов или проблем, связанных с использованием учетных записей домена или АС сотрудник обязан уведомить руководителя структурного подразделения образовательного учреждения и обратиться к администратору домена или АС.

V. Временные учетные записи

29. Для предоставления временного доступа к ресурсам АС образовательного учреждения используется процедура предоставления временных учетных записей.

30. Временная учетная запись – учетная запись, имеющая ограничение по времени действия и ограниченный набор прав использования ресурса. Для временных учетных записей проводится подробное протоколирование их использования. Процедура получения временных учетных:

сотрудник образовательного учреждения оформляет заявку на предоставление временного доступа к информационным, программным и аппаратным ресурсам образовательного учреждения. В заявке указываются: временной интервал использования временной учетной записи, сведения о лице (ФИО, место работы), которое будет использовать временную учетную запись, права, необходимые для такой учетной записи. Заявка утверждается руководителем структурного подразделения образовательного учреждения и направляется на согласование в управление информационной безопасности (ответственный за информационную безопасность);

после согласования управлением информационной безопасности (ответственный за информационную безопасность) образовательного учреждения, заявка направляется оператору ресурса, к которому необходимо предоставить доступ;

временная учетная запись создается оператором ресурса, реквизиты учетной записи передаются заявителю с соблюдением установленных в образовательном учреждении требований по безопасности конфиденциальной информации;

пользователь, получивший временную учетную запись, информируется об ограничениях, связанных с ее использованием;

при необходимости пользователь может оформить заявку с просьбой продлить срок действия временной учетной записи с кратким объяснением причин такой необходимости.

VI. Безопасность привилегированных учетных записей

31. К привилегированным учетным записям относятся учетные записи, используемые для управления работой АС (учетные записи администраторов).

32. При использовании привилегированных учетных записей необходимо руководствоваться принципом «минимальных привилегий», т.е. привилегии администратора должны использоваться только

администратором и только если выполняемая задача требует наличия таких привилегий.

33. Недопустимо использование привилегированных учетных записей в повседневной работе, не связанной с необходимостью их использования (установка, конфигурирование, восстановление операционной системы, сервисов и т.п.).

34. Учетная запись администратора домена может использоваться только при установке, конфигурировании, восстановлении контроллера домена и иных действиях, при которых использование других учетных записей невозможно. Для этой учетной записи проводится подробное протоколирование всех событий ее использования, а также немедленное расследование любого нецелевого ее использования.

35. Для служб и сервисов используется принцип «минимальных привилегий», т.е. службы и сервисы функционируют с минимально возможными для их корректной работы привилегиями.

36. К учетным записям серверов высокой степени критичности (контроллеры домена, серверы баз данных, иные серверы, от которых зависит бесперебойная работа АС образовательного учреждения предъявляются повышенные требования к привилегиям удаленного доступа.

37. В случае компрометации, либо подозрения на компрометацию привилегированной учетной записи проводится внеплановая смена паролей всех зависящих от нее учетных записей.

VII. Аппаратные средства аутентификации

38. Для повышения степени защиты критически важных объектов АС образовательного учреждения (рабочие станции и мобильные компьютеры с информацией высокой степени конфиденциальности, иные объекты) от несанкционированного доступа возможно использование двухфакторной аутентификации (по паролю и предмету – далее ключевой носитель информации).

39. Каждому пользователю АС образовательного учреждения, для которого предусмотрена двухфакторная аутентификация, выдается персональный ключевой носитель информации, который учитывается управлением информационной безопасности(ответственный за информационную безопасность) образовательного учреждения установленным образом (однозначное сопоставление ключевого носителя и его владельца).

40. Ключевые носители информации маркируются управлением информационной безопасности (ответственный за информационную безопасность) образовательного учреждения установленным образом (уникальный номер ключевого носителя) или используется серийный номер производителя.

41. В случае прекращения необходимости использования персонального ключевого носителя (увольнение сотрудника, прекращение функционирования объекта, для аутентификации на котором носитель использовался и т.п.) информация с данного носителя удаляется

установленным образом, либо уничтожается сам носитель в случае невозможности его очистки.

42. Пользователям АС образовательного учреждения категорически запрещается оставлять без личного присмотра ключевые носители, сообщать коды от персонального ключевого носителя, если таковые имеются.

43. Передача ключевого носителя пользователем третьему лицу допускается только при оформлении доверенности в письменной форме с указанием допустимых действий с данным носителем (хранение, использование). Доверенность должна содержать сведения, позволяющие определить:

лиц передающего и получающего ключевой носитель;

цель передачи/получения ключевого носителя;

допустимые действия с ключевым носителем, которые получающая сторона может выполнять с ключевым носителем;

срок, в течении которого получающая сторона в праве совершать указанные действия с ключевым носителем.

44. В случае утраты персонального ключевого носителя пользователь (доверенное лицо) обязан немедленно сообщить об инциденте руководителю структурного подразделения и ответственному за информационную безопасность. При возникновении подобного инцидента необходимо незамедлительно принять меры для недопущения несанкционированного использования утраченного персонального ключевого носителя.

VIII. Контроль

45. Повседневный контроль за соблюдением требований настоящего Положения осуществляется операторами системы обнаружения и предотвращения вторжений путем мониторинга процессов использования и изменения учетных записей, доступа к ресурсам и АС.

46. Ответственный за информационную безопасность проводит ежеквартальный выборочный контроль за соблюдением сотрудниками требований настоящего Положения. О фактах несоответствия качества паролей или условий обеспечения их сохранности ответственный за информационную безопасность сообщает директору образовательного учреждения в форме служебной записки.

IX. Ответственность

48. Пользователи АС образовательного учреждения несут персональную ответственность за несоблюдение требований настоящего Положения.

49. Форма и размер ответственности определяются исходя из вида и размера ущерба, нанесенного ресурсам АС образовательного учреждения действиями либо бездействием соответствующего работника.

государственное автономное профессиональное образовательное учреждение «медногорский индустриальный колледж» г.медногорска оренбургской области (ГАПОУ МИК)

Разработчик:
Администратор
информационной безопасности Горелов С.Н.

Согласовано:
Зам. директора по БОП В.А.Малин