Подписано цифровой подписью: Репина Светлана Николаевна
DN: cn=Репина Светлана Николаевна, o=КОГПОАУ "Вятский торгово-промышленный техникум", ou=директор, email=kirs@profi24.kirov.ru, c=RU
Дата: 2023.03.07 14:47:29 +03'00'

УТВЕРЖДАЮ
Директор КОГПОАУ ВТПТ
_____ Репина С.Н.
Приказ № 119 от "7" 12 2020 г.

Политика назначения и смены паролей в КОГПОАУ «Вятский торгово-промышленный техникум»

Настоящая Политика назначаения и смены паролей (далее – Политика) определяет порядок обеспечения надежных средств идентификации и проверки подлинности пользователей и администраторов, хранящих и обрабатывающих конфиденциальную информацию на автоматизированных рабочих местах (далее – АРМ) и серверах.

1. Ответственным за обеспечение выполнения настоящей политики является Администратор безопасности средств защиты конфиденциальной информации и персональных данных (далее – Администратор безопасности).

2. Установку первичного пароля производит Администратор безопасности при создании новой учётной записи. Ответственность за сохранность первичного пароля лежит на администраторе безопасности.

3. При создании первичного пароля Администратор безопасности обязан установить опцию, требующую смену пароля при первом входе в систему, а также уведомить владельца учётной записи о необходимости произвести смену пароля.

4. Первичный пароль не используется при сбросе забытого пароля на учётную запись, необходима установка нового пароля.

5. Установку основного пароля производит пользователь при первом входе в систему с новой учётной записью.

6. Личные пароли должны выбираться Администраторами и пользователями с учетом следующих требований:

6.1. длина пароля не менее восьми символов;

6.2. пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ, числа, сочетания цифр и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

6.3. пароль не должен содержать имени учетной записи пользователя или частей полного имени пользователя длиной более двух рядом стоящих знаков;

6.4. содержать знаки трех из четырех перечисленных категорий: латинские заглавные буквы (от A до Z), латинские строчные буквы (от a до z), цифры (от 0 до 9), отличающиеся от букв и цифр знаки (например, !, $, #, %);

6.5. при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4-х позициях.

7. Пользователь несёт персональную ответственность за сохранение в тайне основного пароля.

8. Пользователям запрещается:

8.1. записывать пароль и хранить его в легко доступных местах, в том числе на мониторе, рабочем столе или ящиках стола;

8.2. сообщать пароль другим лицам;

8.3. пересылать открытым текстом в электронных сообщениях;

8.4. подбирать пароли других пользователей.

9. Пользователи обязаны сообщать Администратору безопасности о всех случаях попыток противоправных действий пользователей в отношении других пользователей.

10. Полная плановая смена паролей должна проводиться регулярно, не реже одного раза в шесть месяцев для пользователей и не реже одного раза в двенадцать месяцев для администраторов и других технологических учетных записей.

11. Внеплановая смена личного пароля или удаление учетной записи пользователя в случае прекращения его полномочий организации (увольнение, перевод на другую должность) должна производиться Администратором безопасности немедленно после окончания последнего сеанса работы данного пользователя с системой.

12. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, перевод на другую должность) Администратора безопасности.

13. В случае компрометации личного пароля пользователя автоматизированной системы должны быть немедленно предприняты меры в соответствии с пунктами 11 или 12 настоящей Политики в зависимости от полномочий владельца скомпрометированного пароля.

14. Хранение сотрудником (исполнителем) значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе Администратора безопасности.

15. При возникновении нештатных ситуаций, форс-мажорных обстоятельств, которые влекут необходимость доступа к информации пользователя, отсутствующего на рабочем месте, по решению Руководителя может быть инициирован сброс пароля данного пользователя Администратором безопасности и осуществлен доступ к необходимой информации. По факту такого доступа составляется акт, описывающий условия осуществления доступа, который подписывается Руководителем, Администратором безопасности и сотрудником, запросившим доступ.

16. Пользователи должны быть ознакомлены под роспись с настоящей инструкцией. Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на Администратора безопасности.

_____

ЛИСТ ОЗНАКОМЛЕНИЯ
с Политикой назначения и смены паролей

№ п/п	ФИО	Дата	Подпись
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			
26			
27			
28			
29			
30			
31			
32			
33			
34			
35			