Приложение 3
к приказу директора
ГБПОУ КК УТМиПТ
от 27.03.2024 г. № 66

ПОЛИТИКА
использования аутентификационной информации при доступе к информационным ресурсам и системам государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий»

1. Общие положения

1.1. Политика использования аутентификационной информации при доступе к информационным ресурсам и системам (далее – Политика) государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий» (далее – образовательная организация) определяет требования к комплексу мер по использованию аутентификационной информации при реализации доступа к автоматизированным рабочим местам пользователей (далее – АРМ), серверам, активному сетевому оборудованию и средствам защиты информации министерства.

1.2. Под аутентификационной информацией понимается информация, используемая пользователями и администраторами информационных ресурсов (систем) и средств обработки информации для доступа к ним (имя пользователя, пароль, средства дополнительной аутентификации).

1.3. Настоящая Политика разработана в соответствии с:

1.3.1 приказом Федеральной службы по техническому и экспортному контролю России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

1.3.2 приказом Федеральной службы по техническому и экспортному контролю России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

1.3.3 методическим документом Федеральной службы по техническому и экспортному контролю России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах».

2. Порядок формирования и использования аутентификационной информации

2.1. Для обеспечения возможности однозначного сопоставления идентификатора пользователя с запускаемыми от его имени процессами каждому пользователю формируется имя пользователя.

2.2. Для обеспечения возможности однозначного сопоставления устройства доступа (далее – АРМ пользователя) с информационными ресурсами (системами) и средствами обработки информации, к которым осуществляется доступ (объектами доступа), его имя должно соответствовать имени пользователя.

2.3. В случае привлечения третьих лиц для выполнения работ по настройке и тестированию информационных ресурсов (систем) и средств обработки информации, им предоставляются временные учетные записи с предустановленным сроком их действия (при наличии технической возможности), доступ к которым блокируется по завершению работ.

2.4. При создании учетной записи должен быть задан тип учетной записи (при наличии технической возможности). Под типами учетных записей понимается:

2.4.1 учетная запись пользователя;

2.4.2 учетная запись администратора;

2.4.3 временная учетная запись;

2.4.4 системная учетная запись.

2.5. Использование гостевых учетных записей запрещено.

2.6. Локальная учетная запись администратора операционной системы Windows (Administrator) предназначена только для служебного использования администратором при настройке систем и не может быть использована для повседневной работы.

2.7. Учетные записи пользователей не подлежат удалению в системе и могут быть только заблокированы.

2.8. Работники обязаны хранить в секрете персональные пароли доступа к информационным ресурсам (системам) и средствам обработки информации и не передавать их другим лицам. Передача личного пароля пользователя третьим лицам возможно только в случаях, регламентированных в пункте 2.9 настоящей Политики.

2.9. В случае необходимости при проведении проверочных мероприятий (внутренний аналитический аудит), которые требуют знания пароля пользователя, допускается раскрытие значений своего пароля проверяющему сотруднику. По окончанию проверочных работ работники самостоятельно производят немедленную смену значений «раскрытых» паролей.

2.10. В случае возникновении нештатных ситуаций, форс-мажорных обстоятельств, а также технологической необходимости использования имен и паролей работников (в их отсутствие) допускается изменение паролей администратором данного информационного ресурса (системы), средства обработки информации.

2.11. Работники, чьи пароли были изменены, обязаны сразу же после выяснения факта смены своих паролей, создать их новые значения в соответствии с требованиями настоящей Политики.

2.12. Хранение работником (администратором, пользователем) аутентификационной информации допускается только в личном сейфе (запираемом шкафу, ящике) либо в сейфе (запираемом шкафу, ящике) администратора соответствующей информационной системы. При этом бумажный носитель должен быть упакован в отдельный опечатанный конверт.

2.13. При доступе к средствам обработки информации (серверам, активному сетевому оборудованию, средствам защиты информации) запрещается использование аутентификационной информации, заданной производителем «по умолчанию».

2.14. После получения доступа к информационному ресурсу (системе), средству обработки информации пользователь при первом входе в систему должен сменить пароль доступа (в случае наличия технической возможности), на пароль, удовлетворяющий требованиям настоящей Политики.

2.15. При вводе аутентификационной информации (пароля) должно обеспечиваться исключение отображения вводимой парольной информации (например, осуществляется замена вводимых символов условными знаками «-», «*» или иными знаками). В случае отсутствия технической возможности реализации данного требования пользователь самостоятельно создает условия защиты, вводимой аутентификационной информации.

2.16. Запрещается передача аутентификационной информации пользователям при помощи почтовых сообщений, либо по иным открытым каналам связи.

2.17. В случае компрометации аутентификационных данных работники должны незамедлительно сообщить об этом событии, являющемся инцидентом информационной безопасности, Администратору информационной безопасности.

2.18. Предусматривается периодическая плановая (в соответствии с установленным сроком) и внеплановая смена паролей.

2.19. Внеплановая немедленная смена пароля обязательна в случае его компрометации. Также, внеплановая смена пароля и (или) блокирование учетной записи пользователя производится в случае прекращения его полномочий, непосредственно после окончания последнего сеанса работы данного пользователя.

2.20. Должностным лицам запрещается разглашать пароли, ставшие известными им в ходе служебной деятельности по обеспечению функционирования информационных систем.

3. Требования к качеству аутентификационной информации и мер по обеспечению ее безопасности

3.1. К аутентификационной информации пользователей и администраторов информационных ресурсов (систем) и средств обработки информации определены следующие требования, представленные в таблице 1.

Таблица 1 – Требования к аутентификационной информации

№ п/п	Параметр качества пароля	Администратор	Пользователь
1	2	3	4
1	Минимальная длина пароля в символах	12	8
2	Максимальная длина пароля в символах	не ограничена	не ограничена
3	Содержание в пароле букв верхнего и нижнего регистра	да	да
4	Содержание в пароле специальных символов (@, #, $, &, * и тому подобное) и цифр (при наличии технической возможности)	обязательно	рекомендуется
5	Содержание в пароле личных имен, фамилий, кличек домашних животных, номеров телефонов, дат рождения, географических названий, именований АРМ и тому подобное.	запрещено	запрещено
6	Содержание в пароле общепринятых сокращений (Admin, Administrator, ViPNet, Cisco, User, UserID и так далее)	запрещено	запрещено
7	Максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки	3	5
8	Блокировка сеанса доступа в информационную систему после времени бездействия (неактивности) пользователя (минут)	10	15
9	Блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации	30	15
10	Блокировка учетной записи после периода неиспользования (дней)	60	90
11	Минимальное отличие нового пароля от предыдущего (в позициях)	4	3
12	Количество уникальных паролей, устанавливаемых подряд (в течение установленного срока смены паролей)	не менее 5	не менее 3
13	Максимальный срок действия пароля	60 дней	90 дней
14	Минимальный срок действия пароля	нет	нет

4. Ответственность за исполнение положений настоящей Политики

4.1. Ответственность за исполнение положений настоящей Политики возлагается на всех работников образовательной организации, осуществляющих работу на средствах вычислительной техники.

4.2. Пользователи информационных ресурсов и (или) систем образовательной организации должны:

4.2.1 в случае самостоятельного формирования пароля доступа к компонентам информационных ресурсов и (или) систем руководствоваться требованиями к качеству аутентификационной информации и мер по обеспечению ее безопасности, установленными положениями настоящей Политики;

4.2.2 в случае получения аутентификационной информации от администратора информационного ресурса и (или) системы осуществить смену пароля пользователя при наличии технической возможности, а в случае отсутствия технической возможности обеспечить условия его сохранности;

4.2.3 следить за сроком действия паролей и своевременно производить их смену, а в случае отсутствия технической возможности обращаться по вопросу их смены к администраторам информационных ресурсам и (или) систем;

4.2.4 не допускать многократного ввода неправильного пароля и блокировки своих учетных записей;

4.2.5 в случае компрометации аутентификационной информации незамедлительно уведомлять администратора информационной безопасности.

4.3 Администратор информационных систем Техникума обязан:

4.3.1 создавать учетные записи пользователей и обеспечивать управление их жизненным циклом в соответствии с требованиями к качеству аутентификационной информации и мерами по обеспечению ее безопасности, установленными положениями настоящей Политики;

4.3.2 своевременно осуществлять блокировку/разблокировку учетной записи пользователя, а также внеплановую смену пароля в случае запросов пользователей (с незамедлительным информированием Администратора информационной безопасности об инциденте информационной безопасности).

4.3.3 руководствоваться положениями настоящей Политики при задании аутентификационной информации на доступ к средствам защиты информации;

4.3.4 устанавливать и централизованно распространять требования к качеству аутентификационной информации и мерам по обеспечению ее безопасности в соответствии с требованиями, установленными положениями настоящей Политики;

4.3.5 управлять (создавать, изменять, удалять, блокировать, разблокировать) учетными записями пользователей, зарегистрированных в подсистеме управления доступом средства защиты информации от несанкционированного доступа;

4.3.6 осуществлять планирование и реализацию контрольных мероприятий по проверке степени выполнения положений настоящей Политики структурными подразделениями образовательной организации;

4.3.7 организовывать процесс управления инцидентами информационной безопасности в части положений настоящей Политики (в соответствии с Политикой управления событиями безопасности информации).

4.3. Лица, виновные в нарушении положений настоящей Политики, могут быть привлечены к дисциплинарной, материальной, гражданско-правовой и административной ответственности.