УТВЕРЖДАЮ
Директор ОБПОУ «КГТТС»
_____ Е.Н.Брежнев
Приказ № 453/о от 30.12.2016 г.

ИНСТРУКЦИЯ
по управлению средствами аутентификации (паролями) и учетными записями пользователей в информационных системах ОБПОУ «КГТТС»

1. Управление средствами аутентификации (паролями) пользователей и устройств

1.1. Общие положения

Данная инструкция призвана регламентировать управление средствами аутентификации, в том числе процедуры хранения, выдачи, инициализации, блокирования средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации.

Средствами аутентификации являются логин, пароль, используемые для получения доступа пользователя, устройства в информационную систему.

Организационное и техническое обеспечение процедуры управления средствами аутентификации возлагается на администратора безопасности информации (далее - Администратор).

1.2. Функции Администратора по управлению средствами аутентификации

Администратор осуществляет следующие функции по управлению средствами аутентификации:

– изменение аутентификационной информации (паролей), заданных их производителями и (или) используемых при внедрении системы защиты информации информационной системы;

– выдача средств аутентификации (паролей) пользователям;

– генерация и выдача начальной аутентификационной информации (начальных значений средств аутентификации, паролей);

– установление следующих характеристик пароля:

а) задание минимальной сложности пароля с определяемыми оператором требованиями к регистру, количеству символов, сочетанию букв верхнего и нижнего регистра, цифр и специальных символов;

б) задание минимального количества измененных символов при создании новых паролей;

в) задание максимального времени действия пароля;

г) задание минимального времени действия пароля;

д) запрет на использование пользователями определенного оператором числа последних использованных паролей при создании новых паролей;

– блокирование (прекращение действия) и замена утерянных, скомпрометированных или поврежденных средств аутентификации;

– назначение необходимых характеристик средств аутентификации (в том числе механизма пароля);

– обновление аутентификационной информации (замена средств аутентификации) с периодичностью, установленной оператором;

– защита аутентификационной информации от неправомерного доступа к ней и модифицирования.

1.3. Осуществление хранения и учета сведений об аутентификационной информации

Учет средств аутентификации (паролей) на автоматизированных рабочих местах (ПК) ведется в журнале учета средств аутентификации (паролей) пользователей и устройств (далее - Журнал) по форме согласно Приложению №1 к настоящей инструкции.

Журнал содержит таблицу с графами следующего содержания:

– Дата выдачи пароля/токена;
– Сведения об использовании (инв.№ПК, наименование ПО);
– Ф.И.О. Пользователя;
– Пароль/зав.№ токена;
– Подпись администратора;
– Подпись Пользователя;
– Примечание.

За ведение журнала ответственность несет администратор безопасности информации (далее - Администратор).

При получении нового пароля или при его изменении, Администратор делает соответствующую запись в журнале, в свою очередь пользователь ставит свою подпись в соответствующей графе.

После формирования/изменения пароля, Администратор выдает пользователю Лист получения пароля по форме согласно Приложению №2 к настоящей инструкции.

При этом Лист получения пароля с предыдущим, ранее полученным паролем, подлежит уничтожению.

Пользователь несет ответственность за сохранность своего пароля. В случае утери, хищения, ознакомления других лиц с паролем пользователя, пользователь обязан сообщить об этом Администратору.

Помимо обязательного периодического изменения паролей, также изменение должно производиться в следующих случаях:

– увольнение пользователя;
– отпуск или болезнь пользователя;
– утеря пароля пользователем;
– компрометация пароля пользователем;
– изменении прав доступа пользователя к конфиденциальной информации.

В этих случаях смена пароля производится по решению руководителя, с отметкой в графе «Примечание» журнала.

Внеплановая полная смена паролей всех пользователей должна производиться

в случае прекращения полномочий администраторов и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой.

Владельцы паролей должны быть ознакомлены с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

1.4. Требования к характеристикам пароля

Пароли, применяемые в информационных системах, должны соответствовать следующим характеристикам:

– длина пароля не менее 6 символов;

– алфавит пароля не менее 60 символов;

– максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 10 попыток;

– блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 5 до 30 минут;

– смена паролей не более чем через 120 дней.

2. Управление учетными записями пользователей информационных систем

2.1. Общие положения

Данная инструкция призвана регламентировать управление (заведение, активация, блокирование, уничтожение) учетными записями пользователей.

Организационное и техническое обеспечение процедуры управления учетными записями пользователей возлагается на администратора безопасности информации (далее - Администратор).

2.2. Функции Администратора по управлению средствами аутентификации

Администратор осуществляет следующие функции по управлению учетными записями пользователей:

– определение типа учетной записи (внутреннего пользователя, внешнего пользователя; системная, приложения; гостевая (анонимная), временная и (или) иные типы записей);

– объединение учетных записей в группы (при необходимости);

– верификацию пользователя (проверка личности пользователя, его должностных (функциональных) обязанностей) при заведении учетной записи пользователя;

– заведение, активация, блокирование и уничтожение учетных записей пользователей;

– пересмотр и, при необходимости, корректировка учетных записей пользователей с периодичностью не реже одного раза в год;

– предоставление пользователям прав доступа к объектам доступа

информационной системы, основываясь на задачах, решаемых пользователями в информационной системе и взаимодействующими с ней информационными системами.

В информационных системах запрещается использование гостевых (анонимных) и временных учетных записей пользователей, а также более одной привилегированной учетной записи администратора.

Администратор должен оперативно вносить изменения в учетные записи пользователей в случаях изменения сведений о пользователях, их ролях, обязанностях, полномочиях, ограничениях.

Управление учетными записями пользователей информационных систем, имеющих аттестат соответствия требованиям безопасности информации, осуществляется в соответствии с техническим паспортом информационной системы и аттестационной документацией.

При необходимости внесения изменений в учетные записи пользователей (изменение, заведение, активация, блокирование, уничтожение), изменения согласовываются с органом по аттестации, выдавшим аттестат соответствия.