Государственное профессиональное образовательное учреждение Тульской области «Тульский колледж профессиональных технологий и сервиса» (ГПОУ ТО «ТКПТС»)

УТВЕРЖДАЮ
Директор
_____ С.С. Курдюмов
«_31_» ____01____ 2017 г.

ПОЛОЖЕНИЕ

_31.01._ 2017 г. № _202/2_

По организации парольной защиты

1. **Общие положения**

Данное положение регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей), меры обеспечения безопасности при использовании паролей, а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

Требования настоящего Положения являются неотъемлемой частью комплекса мер безопасности и защиты информации в ГПОУ ТО «ТКПТС».

Требования настоящего Положения распространяются на всех работников подразделений, использующих в работе средства вычислительной техники (включая работу в локальной вычислительной сети ГПОУ ТО «ТКПТС») и должны применяться для всех средств вычислительной техники, эксплуатируемой в ГПОУ ТО «ТКПТС.

2. **Термины и определения**

Автоматизированная система (АИС) - совокупность программных и аппаратных средств, предназначенных для хранения, передачи и обработки данных и информации.

Информационная безопасность (ИБ) – обеспечение защищенности информации (ее конфиденциальности, целостности, доступности) от широкого спектра угроз.

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

Учетная запись - информация о сетевом пользователе: имя пользователя, его пароль, права доступа к ресурсам и привилегии при работе в системе. Учетная запись может содержать дополнительную информацию (адрес электронной почты, телефон и т.п.).

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 случае случайного, ошибочного или несанкционированного использования.

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

Ключевой носитель – электронный носитель (дискета, флэш-накопитель, компакт-диск и т.п.), на котором находится ключевая информация (сертификаты и т.п.).

3. Общие требования к паролям

Личные пароли пользователей должны выбираться с учетом следующих требований:

— длина пароля должна быть не менее 8 символов;

— в числе символов пароля обязательно должны присутствовать буквы, цифры и (или) специальные символы (@, #, $, &, *, % и т.п.);

— пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования рабочих станций и т.д.), а также общепринятые сокращения и термины (qwerty, pa$$w0rd, и т.п.);

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

Пароли служебных и привилегированных учетных записей автоматизированной системы должны выбираться с учетом следующих требований:

— длина пароля должна быть не менее 12 символов;

— в числе символов пароля обязательно должны присутствовать, цифры и (или) специальные символы (@, #, $, &, *, % и т.п.).

— пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования рабочих станций и т.д.), а также общепринятые сокращения и термины (qwerty, pa$$w0rd, и т.п.);

— при смене пароля новый пароль должен отличаться от старого не менее, чем четырьмя символами, расположенными не подряд;

— при создании паролей служебных учетных записей возможно использование специализированного программного обеспечения для генерации сложных для подбора легко

запоминаемых паролей.

4. **Безопасность локальных учетных записей**

Встроенная учетная запись Administrator (Администратор) должна быть защищена паролем.

5. **Безопасность доменных учетных записей**

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

В случае производственной необходимости (командировка, отпуск и т.п.), при проведении проверочных мероприятий, выполняемых сотрудниками отдела информационно-программного обеспечения, требующих знания пароля пользователя, допускается раскрытие значений своего пароля начальникам этих подразделений. По окончанию производственных, или проверочных работ работники самостоятельно производят немедленную смену значений "раскрытых" паролей.

В случае возникновении нештатных ситуаций, форс-мажорных обстоятельств, а также технологической необходимости использования имен и паролей работников (в их отсутствие) допускается изменение паролей сотрудниками отдела информационно-программного обеспечения. В подобных случаях, сотрудники, чьи пароли были изменены, обязаны сразу же после выяснения факта смены своих паролей, создать их новые значения.

Пароли учетных записей пользователей АС должны соответствовать требованиям п. 3 Настоящего Положения.

Внеплановая смена личного пароля или удаление учетной записи пользователя автоматизированной системы в случае прекращения его полномочий (увольнение и т.п.) должна производиться сотрудниками отдела информационно-программного обеспечения немедленно после окончания последнего сеанса работы данного пользователя с системой.

Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на работу в другое подразделение и другие обстоятельства) некоторых сотрудников отдела информационно-программного обеспечения.

В случае компрометации личного пароля пользователя АС либо подозрении на

компрометацию должны быть немедленно предприняты меры по внеплановой смене личного пароля самим пользователем с немедленным информированием сотрудников отдела информационно-программного обеспечения.

Смена забытого пользовательского пароля производится сотрудниками отдела информационно-программного обеспечения на основании сообщения пользователя.

6. Контроль

Повседневный контроль над соблюдением требований данного Положения заключается в контроле процессов использования и изменения учетных записей, процессов доступа к ресурсам, процессов изменения учетных записей и предоставления доступа к ресурсам АС сотрудниками отдела информационно-программного обеспечения.

Контроль за выполнением требований данного Положения возлагается на сотрудников отдела информационно-программного обеспечения.

7. Ответственность

Пользователи АС Организации несут персональную ответственность за несоблюдение требований по парольной защите;

Форма и размер ответственности определяются исходя из вида и размера ущерба, нанесенного ресурсам и действиями либо бездействием соответствующего пользователя.