ФГБОУ ВПО «АЛТАЙСКАЯ ГОСУДАРСТВЕННАЯ ПЕДАГОГИЧЕСКАЯ АКАДЕМИЯ»

УТВЕРЖДАЮ
Ректор
ФГБОУ ВПО
«Алтайская государственная
педагогическая академия»
_____И.Р. Лазаренко
«_ __ _» _____ 2013 г.

Инструкция
по организации парольной защиты
ФГБОУ ВПО «Алтайская государственная педагогическая академия»

Барнаул
2013

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в автоматизированной системе (АС) ФГБОУ ВПО «Алтайская государственная педагогическая академия» (далее – ФГБОУ ВПО «АлтГПА»), а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

Идентификация/аутентификация пользователей осуществляется посредством использования TouchMemory или, при отсутствии технической возможности их использования, паролей.

Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах АС ФГБОУ ВПО «АлтГПА» и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на работника администратора информационной безопасности.

Доступ к информационным активам ФГБОУ ВПО «АлтГПА» должен производиться с использованием персональных учетных записей и периодически сменяемых буквенно-цифровых паролей, удовлетворяющих следующим требованиям:

- пароль содержит не менее восьми символов, включая буквы обоих регистров и цифры;
- не является словом, присутствующим в словарях, или профессиональным термином, в т. ч. набранным в другой раскладке клавиатуры;
- не основывается на семейной, служебной и другой легко доступной информации (фамилии, имена, даты рождения, клички животных, автомобильные и телефонные номера, названия организаций, адреса сайтов и т. п.);
- не содержит легко угадываемые последовательности символов (123456, aaabbb, qwerty, q1w2e3 и т. п.).
- одним из способов создания безопасных, но легко запоминающихся паролей является кодирование стихотворной строки или осмысленного утверждения. Так, пароль, созданный на основе фразы: "Вот один пример надежного и запоминающегося пароля", может быть таким: "VotlPN&ZP".

Временный пароль, создаваемый при заведении учетной записи или смене забытого пароля, должен быть уникальным, передаваться способом, исключающим доступ к нему других лиц, и быть сменен пользователем при первом обращении к активу. Пароли, предустановленные производителем, должны сменяться до начала эксплуатации актива.

По решению администратора информационной безопасности, может применяться резервирование некоторых паролей, таких, как пароли администраторов информационных систем, пароли ответственных должностных лиц, пароли отдельных пользователей, выполняющих важные функции, пароли обеспечивающие работу отдельных сетевых сервисов.

Для резервирования пароля выполняются следующие действия:

- пароль записывается на лист бумаги и заверяется личной подписью;
- лист с записью пароля вкладывается владельцем в конверт. Конверт не должен допускать просмотр записи пароля на просвет. Если конверт недостаточно плотный, в него может быть вложен лист темной бумаги. Конверт заклеивается, при необходимости (для особо важных паролей) - опечатывается;
- на конверте владелец пароля указывает свою должность, фамилию и инициалы, наименование информационного средства, которое защищается

этим паролем, текущие дату и время, при необходимости – другие данные, и заверяет запись личной подписью;

- конверт передается на хранение руководителю структурного подразделения ФГБОУ ВПО «АлтГПА» или лицу, им для этого назначенного и учитывается в специальном разделе Журнала учета паролей. Учетный номер (сквозной по Журналу) проставляется ответственным за хранение на конверте.

Конверты с паролями хранятся в сейфе Администратора информационной безопасности. Ответственный за хранение не реже чем один раз в месяц проверяет их наличие по журналу учета.

При замене пароля конверт передается владельцу пароля, который уничтожает лист с резервным паролем, о чем делается запись в Журнале учета паролей. Новый резервный пароль подготавливает к хранению так, как указано выше. Новый конверт учитывается в Журнале учета паролей отдельной позицией.

Вскрытие конверта с паролем производится по решению начальника структурного подразделения в случае необходимости использования прав доступа его владельца в отсутствие самого владельца. Для вскрытия конверта назначается комиссия не менее чем из трех работников ФГБОУ ВПО «АлтГПА». О вскрытии конверта комиссией составляется акт, утверждаемый директором, который по окончании работы комиссии хранится в сейфе администратора информационной безопасности.

При появлении владельца пароля после факта вскрытия конверта пароль заменяется на новый и вновь сохраняется его копия, как описано выше.

Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в три месяца.

Внеплановая смена личного пароля или удаление учетной записи пользователя автоматизированной системы проводится в случае прекращения его полномочий (увольнение, переход на другую работу внутри территориального органа организации и т.п.) производится администратором информационной безопасности 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 другую работу внутри территориального органа организации и другие обстоятельства) администратора информационной безопасности, (администраторов средств защиты и других работников), которым по роду работы были предоставлены полномочия по управлению парольной защитой подсистем АС.

В случае компрометации личного пароля пользователя автоматизированной системы проводится внеплановая смена пароля в зависимости от полномочий владельца скомпрометированного пароля.

Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на ответственных за информационную безопасность в подразделениях (руководителей подразделений), периодический контроль – возлагается на работников ИО – администраторов средств парольной защиты.

ЗАПРЕЩАЕТСЯ:

- сообщать свой персональный пароль другим лицам или записывать его на материальных носителях, доступных для других лиц (кроме предусмотренных случаев сохранения паролей ключевых учетных записей владельцем информационного актива);
- сохранять пароль в программно-технических средствах в открытом виде или использовать средства его автоматического ввода;

- использовать легко угадываемый алгоритм смены пароля (например, F%1hTR8 -* F%2hTR8 -> F%3hTR8, или F%1hTR8 -* Fl%hTR8 -* F1h%TR8 и др.);
- использовать учетные записи других лиц;
- использовать вне ФГБОУ ВПО «АлтГПА» пароли, совпадающие с паролями доступа к его информационно-технологическим активам;
- использовать в качестве паролей примеры, приведенные в Инструкции.

В зависимости от критичности информационно-технологического актива, его владельцем могут быть установлены более высокие требования к сложности пароля и периодичности смены.

Процессы создания, изменения, использования, блокирования, удаления учетных записей, а также смены паролей должны быть регламентированы, протоколироваться и контролироваться.