УТВЕРЖДЕНО
приказом №_____ от «____» _____2011г.

Порядок выдачи и смены паролей для доступа к информационным системам ГОУ ВПО «Тольяттинский государственный университет»

Согласовано
Первый проректор ТГУ

_____Н.Г. Пудовкина

«___»_____2011г.

Тольятти 2011

Содержание

1. Список сокращений

ИС – Информационная система
ПДн – Персональные данные
ИСПДн – Информационная система персональных данных
БД – База данных
СУБД – Система управления базой данных
ПО – Программное обеспечение
АИСУ – Автоматизированная информационная система управления

2.Область применения

Слабая парольная политика или повсеместное ее несоблюдение приводит к возможности компрометации различных участков информационной системы, и как следствие, позволяет реализовать несанкционированный доступ к информации различного уровня критичности.

Несмотря на недостатки однофакторного способа аутентификации с использованием парольной фразы, данный способ является простым, дешевым и наиболее распространенным методом осуществления аутентичности пользователя в большинстве современных информационных систем. Системными администраторами, администраторами и разработчиками ИС должны применяться механизмы противодействия угрозам компрометации паролей пользователей.

3. Требования к парольной защите

3.1. Не должен содержать имени учетной записи пользователя, или частей полного имени пользователя, длиной более двух рядом стоящих знаков;

3.2. Не допускается выбор пароля, являющегося сочетанием из рядом стоящих символов на клавиатуре;

3.3. Пароль должен содержать не менее 6 буквенно - цифровых символов, содержать латинские строчные и заглавные буквы, цифры;

3.4. Срок действия паролей производится на усмотрение администратора конкретной информационной системы и задается программно или административно;

3.5. Не допускается хранение списков паролей администраторами ИС на бумажных копиях;

3.6. Не допускается передача пароля другому лицу;

3.7. Допускается совпадение пароля пользователя в ИС с паролем на образовательном портале, если пароли на портале не будут храниться в системных таблицах в текстовом виде, в противном случае - не допускается;

3.8. Недопустимо использование администраторами СУБД пустых паролей или предлагающихся по умолчанию;

3.9. При установке ПО администратор должен заблокировать “технологические” учетные записи, используемые для первого входа пользователя в систему или для взаимодействия компонентов программного обеспечения между собой;

3.10. Администраторам ИС в настройках конфигурации ПО в настройках парольной политики определить длину пароля не менее 6 символов, если допускает конфигурация, то задать и другие требования;

3.11. Разработчикам ПО не допускать хранение паролей в системных таблицах в виде открытого текста;

3.12. Администраторам защитить от возможного доступа конфигурационные файлы сетевого оборудования, файлы /etc/shadow операционных систем Unix, системные таблицы СУБД, в том числе – доступные с помощью уязвимостей Web-приложений как источники парольных хэшей;

3.13. Разработчикам, при разработке ПО предусматривать разработку механизмов противодействия автоматическому перебору паролей (ввода CAPTCHA, блокировку учетной записи после определенного числа неуспешных попыток аутентификации и т.п.), для имеющегося ПО с открытым кодом - доработать согласно этих требований;

3.14. Список паролей пользователей на доступ к ИС должен храниться у администратора ИС в зашифрованном виде, возможно использование для этого профильного ПО;

3.15. В случае обнаружения пользователем компрометации пароля немедленно сообщить об этом администратору выдававшему пароль и в отдел собственной безопасности.

3.16. Все действующие в Университете ИС должны иметь возможность настройки требований к паролям, периодичности их смены, возможности смены паролей пользователями самостоятельно после первого входа в систему.

4. Порядок выдачи и смены паролей на доступ к информационным системам

Ниже описывается порядок до внедрения системы управления пользователями АИСУ ТГУ.

4.1. Установку первичного пароля производит системный администратор . **Первичный пароль** - комбинация символов (буквы, цифры, знаки препинания, специальные символы), устанавливаемые системным администратором при создании новой учетной записи, согласно требованиям, описанным выше.

4.1.1. Ответственность за сохранность первичного пароля лежит на системном администраторе.

4.1.2. При создании первичного пароля, системный администратор обязан установить опцию, требующую смену пароля при первом входе в систему, а также уведомить владельца учетной записи о необходимости произвести смену пароля.

4.1.3. Первичный пароль так же используется при сбросе забытого пароля на учетную запись. В любом случае, при использовании первичного пароля все требования настоящего документа сохраняются.

4.2. **Основной пароль –** комбинация символов (буквы, цифры, знаки препинания, специальные символы), известная только сотруднику организации, используемая для подтверждения подлинности владельца учетной записи.

4.2.1. Установку основного пароля производит пользователь при первом входе в систему с новой учетной записью.

4.2.2. При выборе пароля необходимо руководствоваться согласно требованиям, описанным выше

4.2.3. Пользователь несет персональную ответственность за сохранение в тайне основного пароля. Запрещается сообщать пароль другим лицам в том числе сотрудникам ИТ отдела, записывать его, а так же пересылать открытым текстом в электронных сообщениях.

4.2.4. Пользователь обязан в установленные администратором ИС производить смену основного пароля соблюдая требования настоящего документа.

4.2.5. В случае компрометации пароля (либо подозрении на компрометацию) необходимо немедленно сообщить об этом в Отдел собственной безопасности и изменить основной пароль.

4.2.6. Восстановление забытого основного пароля пользователя осуществляется системным администратором путем изменения (сброса) основного пароля пользователя на первичный пароль на основании письменной либо электронной заявки пользователя.

4.2.7. Устная заявка пользователя на изменение пароля не является основанием для проведения таких изменений.

4.2.8. Для предотвращения угадывания паролей системный администратор обязан настроить механизм блокировки учетной записи при трехкратном неправильном вводе пароля.

4.2.9. Разблокирование учетной записи пользователя осуществляется системным администратором на основании заявки владельца учетной записи.

4.3. **Административный пароль** - комбинация символов (буквы, цифры, знаки препинания, специальные символы), известная системному администратору (администратору БД, администратору приложения), используемая при настройке служебных учетных записей, учетных записей служб и сервисов а так же специальных учетных записей.

4.3.1. При выборе административного пароля необходимо руководствоваться согласно требованиям, описанным выше.

4.3.2. Системный администратор несет персональную ответственность за сохранение в тайне административного пароля. Запрещается сообщать пароль другим лицам, в том числе сотрудникам компании, записывать его, а так же пересылать открытым текстом в электронных сообщениях.

4.3.3. Системный администратор обязан не реже одного раза в месяц производить смену административного пароля, соблюдая требования настоящего документа.

После внедрения системы управления пользователями АИСУ ТГУ все действия по получению паролей на доступ к информационным системам производятся в Отделе собственной безопасности.

5. Ответственность

Ответственным за актуализацию настоящего порядка является начальник отдела собственной безопасности, директор ЦНИТ, первый проректор ТГУ

Контроль над исполнением настоящей инструкции возложить на начальника отдела собственной безопасности Басацкого В.В.

6. Список разработчиков и согласования

Начальник
Отдела собственной безопасности В.В. Басацкий

Директор центра
новых информационных технологий В.В. Ефросинин

Список согласования:

Начальник управления делами Е.В. Даценко