Вологодская государственная
молочнохозяйственная академия
им. Н. В. Верещагина

Руководство пользователя
[Инструкция по организации парольной защиты]

Центр ИСТ, 2015

Содержание

Введение

Настоящая инструкция регламентирует организационно-техническое обеспечение генерации, смены и прекращения действия паролей в информационной системы персональных данных, а также контроль за действиями пользователей системы при работе с паролями

Правила формирования личного пароля

1. В качестве пароля должна выбираться случайная последовательность символов, обеспечивающая малую вероятность её подбора. При возможности (см. п. 1.2) в пароль должны быть включены символы верхнего и нижнего регистров, цифры и специальные символы, такие, как “ ~ ! @ # $ % ^ & * ( ) - + _ = \ | / ? , . < >. Длина пароля должна быть не менее 8 символов.
2. При выборе пароля необходимо учитывать ограничения конкретных систем и программ, которые не могут соответствовать таким требованиям (например, не все программы позволяют вводить спецсимволы в пароле или длина пароля может быть ограничена до какого-либо числа символов).
3. Запрещается использовать в качестве пароля «пустой» пароль, имя входа в систему (логин), простые пароли типа «123», «111», «qwerty» и им подобные, общепринятые сокращения (ЭВМ, ЛВС, USSR и т. п.), а так же имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов, паспортов и другие пароли, которые можно угадать, основываясь на информации о пользователе.
4. Запрещается выбирать пароли, которые уже использовались ранее.

Ввод пароля

1. Ввод пароля должен осуществляться с учётом регистра (верхний-нижний), в котором пароль был задан и с учётом текущей раскладки клавиатуры (RU-EN и др.).
2. Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев в прямой видимости или отражённом свете) или техническими средствами (видеокамеры, фотоаппараты и др.).

Порядок смены личных паролей

1. Полная плановая смена паролей должна проводиться регулярно, не реже одного раза в 3 месяца (90 календарных дней).
2. Внеплановая смена (удаление) личного пароля любого пользователя автоматизированной системы в случае прекращения его полномочий (увольнение, либо переход на другую работу внутри академии) должна производиться немедленно после окончания последнего сеанса работы данного пользователя системы.
3. Внеплановая полная смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри академии и другие обстоятельства) администратора информационной безопасности или других сотрудников, которым по роду работы были предоставлены либо полномочия по управлению автоматизированной системой в целом, либо полномочия по управлению подсистемой защиты информации данной автоматизированной системы, а значит, кроме личного пароля им могут быть известны пароли других пользователей системы.
4. Смена личного пароля производится самостоятельно каждым пользователем в соответствии с данной инструкцией.
5. Уполномоченные лица Центра ИСТ оказывают необходимую консультативную помощь пользователям о процессе смены пароля.
6. Изменять заданный администратором временный пароль следует при первом же входе в систему.

Хранение пароля

1. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.
2. Хранение сотрудником (исполнителем) своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у руководителя подразделения в опечатанном конверте.
3. Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

Действия в случае утраты и компрометации пароля

1. В случае утраты пароля сотрудник сообщает об этом начальнику подразделения и получает у администратора системы временный пароль и самостоятельно его изменяет в соответствии с вышеуказанными требованиями.
2. В случае компрометации пароля (подсматривание его кем-либо, разглашение пароля и др.) или подозрения на компрометацию пароль необходимо сменить как можно скорее в соответствии с вышеуказанными требованиями.

Ответственность при организации парольной защиты

1. Ответственность за организацию парольной защиты в подразделениях академии возлагается на уполномоченных лиц Центра ИСТ.
2. Периодический контроль за соблюдением требований данной инструкции возлагается на администратора информационной безопасности.
3. Владельцы паролей должны под расписку быть ознакомлены с данной инструкцией и предупреждены об ответственности за использование паролей не соответствующих требованиям, за ненадлежащее хранение личного пароля, а также за разглашение парольной информации.