УТВЕРЖДАЮ
Ректор ФГБОУ ВПО «НВГУ»
_____ С.И. Горлов
«30» _____ 2013 г.

Инструкция по парольной защите в информационных системах персональных данных

1. Общие сведения

1.1. С целью ограничения доступа к информационной системе обработки персональных данных (ИСПДн) в ФГБОУ ВПО «НВГУ» устанавливается единая система установки паролей на базе встроенного в BIOS общего и прикладного программного обеспечения средств защиты информации.

1.2. Личные пароли должны выбираться пользователями самостоятельно, с учетом следующих требований:

- длина пароля должна быть не менее 6 буквенно-цифровых символов.
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения.
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях.
- количество смен, через которые разрешается повторение предыдущего пароля – не менее 10.
- количество неудачных попыток входа, после которых происходит блокирование – не более 5.

1.3. Личный пароль сотрудника, допущенного к информационным ресурсам ИСПДн, составляет его секрет и разглашению не подлежит.

1.4. Удаление учетной записи пользователя ИСПДн в случае его увольнения должно производиться немедленно после окончания последнего сеанса работы данного пользователя, по представлению служебной записки сотрудником отдела кадров.

1.5. Сетевое имя и индивидуальный пароль являются идентификатором пользователя в ИСПДн.

1.6. При входе в ИСПДн пользователь обязан зарегистрироваться под своим пользовательским именем и набрать индивидуальный пароль, после чего он получает доступ к отведенным для него ресурсам.

1.7. С целью контроля за реализацией прав доступа пользователей к информационным ресурсам ИСПДн должно быть организовано ведение аудита ИСПДн с использованием встроенных механизмов операционной системы и средств защиты информации.

1.8. Действия пользователей, допущенных к информационным ресурсам, хранимым на сервере ИСПДн, могут протоколироваться. Ответственность за уничтожение, изменение информации несет пользователь, под чьим именем операция была зарегистрирована, если в результате расследования не определено конкретное виновное лицо.

1.9. Нарушение пользователями целостности установленного программного обеспечения, а также самовольное установление программ, не предназначенных для выполнения должностных обязанностей, категорически запрещается.

1. Порядок плановой и внеплановой смены личного пароля

1.1. Полная плановая смена паролей должна проводиться регулярно, но не реже одного раза в 6 месяцев.

1.2. Внеплановая смена любого пароля пользователя ИСПДн производится:

- по просьбе самого пользователя.
- по требованию администратора безопасности ИСПДн.

1.3. В случае временного прекращения полномочий пользователя ИСПДн (болезнь, отпуск, командировка и т.п.) администратором безопасности ИСПДн производиться блокировка учетной записи пользователя по представлению служебной записки руководителем структурного подразделения.

1.4. Внеплановая смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и другие обстоятельства) администраторов безопасности ИСПДн и других сотрудников, которым по роду работы были предоставлены либо полномочия по управлению ИСПДн в целом, либо полномочия по управлению системой защиты информации данной ИСПДн, а значит, кроме личного пароля, им были известны пароли других пользователей.

2. Действия при компрометации пароля

2.1. В случае компрометации личного пароля хотя бы одного пользователя ИСПДн смена паролей производится в объеме, зависящем от полномочий владельца скомпрометированного пароля.

2.2. По всем фактам компрометации паролей проводят служебное расследование.

2.3. Каждый пользователь ИСПДн, получает свое пользовательское имя учетной записи, которое составляется администратором безопасности ИСПДн и доводится пользователю.

2.4. Все пользователи ИСПДн, должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, за разглашение парольной информации и сохранность информации на отведенных ему разделах сервера.