МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ПЕРМСКАЯ ГОСУДАРСТВЕННАЯ СЕЛЬСКОХОЗЯЙСТВЕННАЯ
АКАДЕМИЯ ИМЕНИ АКАДЕМИКА Д. Н. ПРЯНИШНИКОВА»

Утверждаю
Ректор
ФГБОУ ВО Пермская ГСХА
Ю.Н. Зубарев _____
«29» _____ 2015 г.

Инструкция
по организации парольной защиты
ФГБОУ ВО Пермская ГСХА

2015

1. Общие положения

Настоящая инструкция устанавливает основные правила введения парольной защиты в ФГБОУ ВО Пермская ГСХА (далее – Академия) и регламентирует организационно-техническое обеспечение генерации, смены и прекращения действия паролей, а также контроль за действиями пользователей системы при работе с паролями. Настоящая инструкция оперирует следующими основными понятиями:

- **Идентификация** - присвоение пользователям и объектам доступа уникального и однозначно определяющего их в пределах ИСПД идентификатора, и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.
- **ИСПД** - информационная система персональных данных.
- **Компрометация** - факт доступа постороннего лица к защищаемой информации, а также подозрение на него.
- **Логин –** идентификатор учетной записи пользователя.
- **Несанкционированный доступ(НСД)** - доступ к информации, нарушающий правила разграничения доступа в ИСПД.
- **Объект доступа –** единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.
- **Пароль** - признак пользователя, предъявляемый совместно с логином в процессе идентификации.
- **Правила доступа** - совокупность правил, регламентирующих права доступа пользователя к объектам доступа.
- **Пользователь** - лицо, действия которого регламентируются правилами разграничения доступа.

2.Правила генерации логинов и паролей

2.1. Логины генерируются специалистами отдела качества и информатизации.

2.2. Персональные пароли генерируются специалистами отдела качества и информатизации. Смена пароля допускается пользователем самостоятельно в соответствии с требованиями данной инструкции.

2.3. Длина пароля должна быть не менее 8 символов.

2.4. В составе пароля должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы.

2.5. Пароль не должен включать в себя:

- номера телефонов, автомобилей;
- персональные данные (ФИО, дата рождения, номер паспорта, номер зачетной книжки, адрес и т.п.);
- при смене пароля новое сочетание символов должно

отличаться от предыдущего не менее чем на 2 символа.

2.6. Допускается использование единого пароля для доступа субъекта доступа к различным информационным ресурсам одной ИСПД.

2.7. Срок действия пароля задается ответственным за безопасность ИСПД. Пользователь обязан сменить пароль по истечению срока его действия.

2.8. Полная плановая смена паролей пользователей проводится по распоряжению ответственного за безопасность ИСПД.

3. Обязанности пользователей при работе с парольной защитой

3.1. При работе с парольной защитой пользователям запрещается:

- разглашать кому-либо персональный пароль и прочие идентифицирующие сведения;
- предоставлять доступ от своей учетной записи к информации, хранящейся в ИСПД, посторонним лицам;
- записывать пароли на бумаге, файле, электронных и прочих носителях информации, в том числе и на предметах.

3.2. Хранение пользователем своего пароля на бумажном носителе допускается только в личном, опечатанном владельцем пароля, сейфе.

3.3. При вводе пароля пользователь обязан исключить возможность его перехвата сторонними лицами и техническими средствами.

4. Компрометация паролей

4.1. Под компрометацией следует понимать следующее:

- физическая утеря носителя с парольной информацией;
- передача идентификационной информации по открытым каналам связи вне ИСПД;
- проникновение постороннего лица в помещение физического хранения носителя парольной информации или алгоритма, или подозрение на него (срабатывание сигнализации, повреждение устройств контроля НСД (слепков печатей), повреждение замков и т. п.);
- визуальный осмотр носителя идентификационной информации посторонним лицом;
- перехват пароля при распределении идентификаторов;
- сознательная передача информации постороннему лицу.

4.2. Действия при компрометации пароля:

- скомпрометированный пароль сразу же выводится из действия, взамен его вводятся запасной или новый пароль.

5. Ответственность пользователей при работе с парольной

защитой

5.1. Повседневный контроль за действиями сотрудников Академии при работе с паролями, соблюдением порядка их смены, хранения и использования, возлагается на отдел качества и информатизации.

5.2. Владельцы паролей должны быть ознакомлены с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

5.3. Ответственность за организацию парольной защиты возлагается на ответственного за безопасность ИСПД.

5.4. Ответственность в случае несвоевременного уведомления ответственного за систему защиты информации в информационной системе персональных данных о случаях утери, кражи, взлома или компрометации паролей возлагается на владельца взломанной учетной записи.