УТВЕРЖДАЮ

Ректор ПГНИУ
_____/Макарихин И.Ю.

«___»_____20__ г.

ИНСТРУКЦИЯ

по организации парольной защиты ИСПД ПГНИУ

1. Общие положения

Настоящая инструкция устанавливает основные правила парольной защиты 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 субъектам 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.
- **Объект доступа** - единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.
- **Пароль –** признак субъекта доступа, предъявляемый совместно с идентификатором субъекта в процессе идентификации.
- **Правила доступа** - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.
- **Субъект доступа** - лицо или процесс, действия которого регламентируются правилами разграничения доступа.
- **Несанкционированный доступ** - доступ к информации, нарушающий правила разграничения доступа в ИСПД.

2. Правила генерации паролей

2.1. Персональные пароли должны генерироваться специальными программными средствами административной службы либо задаваться субъектом самостоятельно в соответствии с требованиями данной инструкции.

2.2. Длина пароля должна быть не менее 12 символов.

2.3. В составе пароля должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы либо пароль должен представлять собой фразу из нескольких слов.

2.4. 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.

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

2.6. Срок действия пароля задается администратором информационной безопасности. Субъект обязан сменить пароль по истечению срока его действия.

3. Порядок смены паролей

3.1. Полная плановая смена паролей пользователей должна проводиться по предложению администратора информационной безопасности ИСПД и на основании распоряжения руководителя структурного подразделения.

3.2. В случае компрометации личного пароля пользователя надлежит немедленно ограничить доступ к информации с данной учетной записи, до момента вступления в силу новой учетной записи пользователя или пароля.

4. Обязанности пользователей при работе с парольной защитой

4.1. 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.

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

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

5. Компрометация паролей

5.1. 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.);
- перехват пароля при распределении идентификаторов;
- сознательная передача информации постороннему лицу.

5.2. Действия при компрометации пароля:
- скомпрометированный пароль сразу же выводится из действия, взамен вводятся запасной или новый пароль;
- о компрометации немедленно оповещаются все участники обмена информацией.

6. Ответственность пользователей при работе с парольной защитой

6.1. Ответственность за организацию парольной защиты возлагается на администратора информационной безопасности ИСПД.

6.2. Повседневный контроль за действиями работников ПГНИУ при работе с паролями, соблюдением порядка их смены, хранения и использования, возлагается на администратора информационной безопасности ИСПД.

6.3. 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.

6.4. Ответственность в случае несвоевременного уведомления ответственного за систему защиты информации в ИСПД о случаях утери, кражи, взлома или компрометации паролей возлагается на владельца взломанной учетной записи.