Федеральное государственное бюджетное образовательное учреждение высшего образования
«Башкирский государственный педагогический Университет им. М.Акмуллы»
(ФГБОУ ВО «БГПУ им.М.Акмуллы»)

ПОРЯДОК

СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

ПОРЯДОК ВЫДАЧИ И СМЕНЫ ПАРОЛЕЙ ДЛЯ ДОСТУПА К ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ в ФГБОУ ВО «БГПУ им.М.Акмуллы»

ПОР–12–10– 2017

Официальное издание

Предисловие

1 ПОРЯДОК РАЗРАБОТАН
ведущим специалистом по администрированию сетевых устройств информационно-технического управления Д.О. Лобаренко _____

2 УТВЕРЖДАЮ
ректор ФГБОУ ВО «БГПУ им. М.Акмуллы» _____ Р.М.Асадуллин

3 ПОРЯДОК ВВЕДЕН В ДЕЙСТВИЕ приказом ректора ФГБОУ ВО «БГПУ им.М.Акмуллы»
от «26» 09. 2017г. № 343/0

Экземпляр № 2.

4 ПОРЯДОК СОГЛАСОВАН

Проректор по УР _____ А.Ф. Мустаев

Проректор по информационным технологиям _____ И.В. Кудинов

Начальник информационно-технического управления _____ Р.Р. Уразаков

Начальник УМУ _____ Г.Р. Гильманова

Начальник отдела кадров _____ С.Д. Камалова

Начальник юридического отдела _____ Э.М. Даянова

Начальник отдела документационного обеспечения _____ Г.Р. Фаттахова

СОДЕРЖАНИЕ:

1 Общие положения

Настоящий порядок устанавливает основные правила введения парольной защиты информационной системы персональных данных в ФГБОУ ВО «БГПУ им. М. Акмуллы» (далее – Университет). Порядок 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. Настоящий порядок оперирует следующими основными понятиями:

- **Идентификация** - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.
- **ИСПДн –** 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** – уникальный признак субъекта доступа, который является его (субъекта) секретом.
- **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** (НСД) - доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированных систем.

2 Правила генерации паролей

2.1 Персональные пароли должны генерироваться специальными программными средствами административной службы.

2.2 Длина пароля должна быть не менее 6 символов.

2.3 В составе пароля рекомендуется использовать буквы в верхнем и нижнем регистрах, цифры и специальные символы.

2.4 Пароль не должен включать в себя:

- легко вычисляемые сочетания символов;
- клавиатурные последовательности символов и знаков;
- общепринятые сокращения;
- аббревиатуры;
- номера телефонов, автомобилей;
- прочие сочетания букв и знаков, ассоциируемые с пользователем;
- 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 ИСПДн объекта Университета.

3 Порядок смены паролей

3.1 Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одно раза в шесть месяцев.

3.2 Полная внеплановая смена паролей всех пользователей должна производиться в случае прекращения полномочий администраторов средств защиты или других сотрудников, которым по роду службы были предоставлены полномочия по управлению парольной зашитой.

3.3 Полная внеплановая смена паролей должна производиться в случае компрометации личного пароля одного из администраторов ИСПДн.

3.4 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 ИСПДн посторонним лицам;
- записывать пароли на бумаге, файле, электронных и прочих носителях информации, в том числе и на предметах к которым могут иметь свободный доступ иные лица.

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

5 Случаи компрометации паролей

5.1 Под компрометацией следует понимать:

- физическая утеря носителя с информацией;
- передача идентификационной информации по открытым каналам связи;
- 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.

5.2 Действия при компрометации пароля:

- скомпрометированный пароль сразу же выводится из действия, взамен его вводятся запасной или новый пароль;
- о компрометации немедленно оповещаются все участники обмена информацией. Пароль вносится в специальные списки, содержащие скомпрометированные пароли и учетные записи.

6 Ответственность пользователей при работе с парольной защитой

6.1 Повседневный контроль за действиями сотрудников Университета при работе с паролями, соблюдением порядка их смены, хранения и использования, возлагается на ответственного за систему защиты информации в информационной системе персональных данных.

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

6.3 Ответственность за организацию парольной защиты возлагается на ответственного за систему защиты информации в информационной системе персональных данных.

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

Лист ознакомления с порядком выдачи и смены паролей для доступа к ИСПДн в ФГБОУ ВО «БГПУ им. М. Акмуллы»

№ п/п	Фамилия, имя, отчество сотрудника	Дата ознакомления с Порядком	Подпись сотрудника