

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 ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ
ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ С
ИСПОЛЬЗОВАНИЕМ СРЕДСТВ АВТОМАТИЗАЦИИ
в ФГБОУ ВО «БГПУ им.М.Акмуллы»**

ПОР-12-07- 2017

Официальное издание

Порядок не может быть полностью или частично воспроизведено,
тиражировано и распространено без письменного разрешения
ректора ФГБОУ ВО «БГПУ им.М.Акмуллы».

Предисловие

1 ПОРЯДОК РАЗРАБОТАН

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

2 УТВЕРЖДАЮ

ректор ФГБОУ ВО «БГПУ им. М.Акмиллы» _____ Р.М.Асадуллин

3 ПОРЯДОК ВВЕДЕН В ДЕЙСТВИЕ приказом ректора ФГБОУ ВО «БГПУ
им.М.Акмиллы»

от «26» 09.2017 № 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:

Общие положения	4
Лист ознакомления с порядком обеспечения безопасности при обработке персональных данных, осуществляемой с использованием средств автоматизации в ФГБОУ ВО «БГПУ им. М. Акмуллы»	6

1. Общие положения

Обработка персональных данных с использованием средств автоматизации означает совершение действий (операций) с такими данными с помощью объектов вычислительной техники в Корпоративной компьютерной сети Университета (далее - ККС).

Безопасность персональных данных при их обработке в ККС обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, а также используемые в ККС информационные технологии.

Технические и программные средства защиты информации должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации. Средства защиты информации, применяемые в ККС, в установленном порядке проходят процедуру оценки соответствия.

Допуск лиц к обработке персональных данных с использованием средств автоматизации осуществляется на основании "Политики информационной безопасности" при наличии ключей (паролей) доступа.

Работа с персональными данными в ККС должна быть организована таким образом, чтобы обеспечивалась сохранность носителей персональных данных и средств защиты информации, а также исключалась возможность неконтролируемого пребывания в этих помещениях посторонних лиц.

Компьютеры и (или) электронные папки, в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены индивидуальными паролями доступа, состоящими из 6 и более символов. Работа на компьютерах с персональными данными без паролей доступа, или под чужими или общими (одинаковыми) паролями, запрещается.

Пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в том числе Интернет, запрещается.

При обработке персональных данных в ККС пользователями должно быть обеспечено:

- использование предназначенных для этого разделов (каталогов) носителей информации, встроенных в технические средства, или съемных маркированных носителей;
- недопущение физического воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- недопущение несанкционированного выноса из помещений, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

При обработке персональных данных в ККС разработчиками и администраторами систем должны обеспечиваться:

- обучение лиц, использующих средства защиты информации, применяемые в ККС, правилам работы с ними;
- учет лиц, допущенных к работе с персональными данными в ККС, прав и паролей доступа;
- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;
- контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- описание системы защиты персональных данных.

Специфические требования по защите персональных данных в отдельных автоматизированных системах Университета определяются утвержденными в установленном порядке инструкциями по их использованию и эксплуатации.

