

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

ИНСТРУКЦИЯ

СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

ИНСТРУКЦИЯ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЙ ИНФОРМАЦИОННОЙ
СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ в
ФГБОУ ВО «БГПУ им.М.Акмуллы»

И-12-12- 2017

Официальное издание

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

Предисловие

1 ИНСТРУКЦИЯ РАЗРАБОТАНА

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 ИНСТРУКЦИЯ ВВЕДЕНА В ДЕЙСТВИЕ приказом ректора ФГБОУ ВО «БГПУ им.М.Акмиллы»

от «26» 09.2017 № 343/0

Экземпляр № 2.

4 ИНСТРУКЦИЯ СОГЛАСОВАНА

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
Должностные обязанности	5
Организация парольной защиты	7
Правила работы в сетях общего доступа и (или) международного обмена	8
Права и ответственность пользователей ИСПДн	9

1. Общие положения

1.1. Пользователь информационных систем персональных данных (ИСПДн) (далее – Пользователь) осуществляет обработку персональных данных (ПДн) в информационной системе персональных данных.

1.2. Пользователем является каждый сотрудник ФГБОУ ВО «БГПУ им. М. Акмуллы» (далее - БГПУ им. М. Акмуллы), участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.3. Пользователь несет персональную ответственность за свои действия.

1.4. Пользователь в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами Федеральной службы по техническому и экспортному контролю России (ФСТЭК) и регламентирующими документами БГПУ им. М. Акмуллы.

1.5. Методическое руководство работой пользователя осуществляется ответственным за обеспечение защиты персональных данных.

2. Должностные обязанности

Пользователь обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.2. Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него в Положении о разграничении прав доступа к обрабатываемым персональным данным.

2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.

2.4. Соблюдать требования парольной политики.

2.5. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена – Интернет и других.

2.6. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью БГПУ им. М. Акмуллы, а так же для получения консультаций по вопросам информационной безопасности, необходимо обратиться к ответственному лицу по информационной безопасности.

2.8. Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к Администратору ИСПДн по внутреннему телефону.

2.9. Пользователям запрещается:

- разглашать защищаемую информацию третьим лицам;
- копировать защищаемую информацию на внешние носители без разрешения своего руководителя;
- самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;
- несанкционированно открывать общий доступ к папкам на своей рабочей станции;
- запрещено подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства;
- отключать (блокировать) средства защиты информации;
- обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн;
- сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн;

– привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных.

2.10. При отсутствии визуального контроля за рабочей станцией доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt> и выбрать опцию <Блокировка>.

2.11. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в пределах возложенных на него функций.

3. Организация парольной защиты

3.1 Личные пароли доступа к элементам ИСПДн выдаются пользователям ответственным лицом по информационной безопасности, Администратором ИСПДн или создаются самостоятельно.

3.2. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 6 месяца.

3.3. Правила формирования пароля:

- пароль не может содержать имя учетной записи пользователя или какую-либо его часть.

- пароль должен состоять не менее чем из 8 символов.

- в пароле должны присутствовать символы трех категорий из числа следующих четырех:

- прописные буквы английского алфавита от А до Z;

- строчные буквы английского алфавита от а до z;

- десятичные цифры (от 0 до 9);

- запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а так же имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе;

- запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

- запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

- запрещается выбирать пароли, которые уже использовались ранее.

3.4. Правила ввода пароля:

- ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан;

- во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

3.5. Правила хранения пароля:

- запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;

- запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

3.6. Лица, использующие паролирование, обязаны:

- четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию;

- своевременно сообщать Администратору информационной безопасности об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

4. Правила работы в сетях общего доступа и (или) международного обмена

4.1. Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее – Сеть) на элементах ИСПДн, должна проводиться при служебной необходимости.

4.2. При работе в Сети запрещается:

- осуществлять работу при отключенных средствах защиты (антивирус и других);
- передавать по Сети защищаемую информацию без использования средств шифрования;
- запрещается скачивать из Сети программное обеспечение и другие файлы;
- запрещается посещение сайтов сомнительной репутации (порно-сайты, сайты, содержащие нелегально распространяемое программное обеспечение и другие);
- запрещается нецелевое использование подключения к Сети.

5. Права и ответственность пользователей ИСПДн

5.1 Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн.

5.2 Пользователи, виновные в несоблюдении Настоящей инструкции расцениваются как нарушители Федерального закона РФ 27.07.2006 г. N 152-ФЗ "О персональных данных" и несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.