Приложение № 3

**ИНСТРУКЦИЯ ПО РАБОТЕ ПОЛЬЗОВАТЕЛЕЙ
ИСПДН ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМ. В.Г. ШУХОВА»**

**2021 г.**

# Настоящая инструкция определяет общие положения работы пользователей в защищенной от несанкционированного доступа аттестованного по требованиям безопасности информации ИСПДн.

1. Допуск пользователей к работе в ИСПДн осуществляется в соответствии с утверждаемым списком лиц, допущенных к работе на АРМ в ИСПДн.

2. Учет работы пользователей в ИСПДн производится в электронном журнале обращений.

3. Пользователь имеет право решать поставленные задачи в соответствии с полномочиями доступа к ресурсам в ИСПДн, присвоенными администратором безопасности данному пользователю.

4. Присвоение пользователю полномочий доступа к ресурсам компьютера и определение возможного времени работы пользователя на АРМ осуществляется администратором ИСПДн при первичной регистрации пользователя.

5. Пользователь отвечает за правильность включения и выключения технических средств, входящих в состав ИСПДн, входа в систему и все действия при работе в ней.

6. В процессе первичной регистрации для работы на АРМ пользователь заявляет администратору ИСПДн перечень необходимых для его работы ресурсов и состав необходимого общесистемного программного обеспечения для решения поставленных задач.

7. Вход пользователя в систему осуществляется на основе предъявления имени, присвоенного при первичной регистрации администратором ИСПДн и ввода личного пароля, закреплённого за конкретным пользователем.

8. В целях предотвращения несанкционированного доступа посторонних лиц к ресурсам пользователя осуществляется периодическая (раз в три месяца) замена пароля постоянного пользователя. Замена личного пароля осуществляется пользователем самостоятельно. В случае отказа системы в идентификации пользователя либо неподтверждения личного пароля следует немедленно обратиться к администратору ИСПДн.

9. Резервное копирование, уничтожение и восстановление информации осуществляются пользователем в рамках выделенных полномочий, либо через администратора ИСПДн. Пользователь осуществляет резервное копирование информации в процессе, либо по окончании работы на ЖМД.

10. При работе со съёмными магнитными носителями пользователь каждый раз перед началом работы обязан проверить их на наличие вирусов с использованием штатных антивирусных программ, установленных на АРМ, в соответствии с «Инструкцией по организации антивирусного контроля». В случае обнаружения вирусов пользователь обязан немедленно сообщить администратору ИСПДн.

11. В процессе работы пользователю запрещается:

* + использовать для постоянного хранения и обработки конфиденциальной информации неучтенные съемные носители, за исключением тех, которые были учтены;
	+ самовольно вносить какие-либо изменения в состав, размещение и конфигурацию средств автоматизированной системы или устанавливать дополнительно любые программные и аппаратные средства;
	+ осуществлять попытки несанкционированного доступа к ресурсам системы и других пользователей;
	+ использовать в ИСПДн неучтенные съемные носители USB-флэш электронные накопители;
	+ оставлять не запертым помещение с включенными техническими средствами до окончания работы;
	+ не допускать присутствия посторонних лиц в помещении, где находятся АРМ ИСПДн.

12. В случае возникновения сбоев в работе на АРМах в ИСПДн необходимо обращаться к администратору ИСПДн, администратору безопасности.

|  |  |  |
| --- | --- | --- |
| **Начальник управления информатизации и коммуникаций** |  | **И.Н. Гвоздевский** |