МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» (ФГБОУ ВО «ВГТУ», ВГТУ)**

**УТВЕРЖДАЮ**
**Ректор ВГТУ**
**_____ В.Р. Петренко**
**«_10_» _____ 2016 г.**

Система менеджмента качества

# РУКОВОДСТВО АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

Воронеж 2016

1 РАЗРАБОТАНО рабочей группой.

2 ОТВЕТСТВЕННЫЙ ИСПОЛНИТЕЛЬ начальник ОИСК Д.В. Макаров

3 УТВЕРЖДЕНО И ВВЕДЕНО В ДЕЙСТВИЕ приказом ректора ВГТУ
от 10.02.2016 № 05–01.18–0

4 ВВОДИТСЯ ВПЕРВЫЕ

## 1. Общие положения.

1.1. Настоящее Руководство определяет права, обязанности, задачи, функции администратора безопасности информационной системы «Университет» (далее – ИСПДн).

## 2. Обязанности администратора безопасности.

2.1. Знать и выполнять требования законодательства РФ и локальных актов Организации, устанавливающих правила обработки и защиты персональных данных (далее – ПДн) в ИСПДн.

2.2. При эксплуатации ИСПДн с целью защиты ПДн администратор безопасности обязан:

2.2.1. Выполнять и принимать меры к выполнению требований следующих документов:

2.2.1.1. «Инструкция по идентификации, аутентификации пользователей информационной системы персональных данных»;

2.2.1.2. «Инструкция по управлению доступом к персональным данным»;

2.2.1.3. «Инструкция по управлению программным обеспечением»;

2.2.1.4. «Инструкция по защите машинных носителей персональных данных»;

2.2.1.5. «Инструкция по управлению событиями информационной безопасности»;

2.2.1.6. «Инструкция по антивирусной защите»;

2.2.1.7. «Инструкция по контролю защищенности персональных данных»;

2.2.1.8. «Инструкция по защите технических средств информационной системы персональных данных»;

2.2.1.9. Настоящее Руководство.

2.2.2. Знать и выполнять требования внутреннего регламента ВГТУ.

2.2.3. Осуществлять установку, настройку и сопровождение технических средств защиты.

2.2.4. Участвовать в контрольных и тестовых испытаниях и проверках элементов ИСПДн.

2.2.5. Участвовать в приемке новых программных средств.

2.2.6. Обеспечить доступ к защищаемой информации пользователям ИСПДн согласно их правам доступа при получении оформленного соответствующим образом разрешения.

2.2.7. Уточнять в установленном порядке обязанности пользователей ИСПДн по обработке персональных данных.

2.2.8. Вести контроль над процессом осуществления резервного копирования персональных данных.

2.2.9. Анализировать состояние защиты ИСПДн и ее отдельных подсистем и докладывать результаты анализа ответственному за организацию обработки ПДн.

2.2.10. Контролировать неизменность состояния средств защиты их параметров и режимов защиты. При возникновении отклонений докладывать ответственному за организацию обработки ПДн.

2.2.11. Контролировать физическую сохранность технических средств ИСПДн и средств защиты информации (далее – СЗИ). О нарушениях докладывать ответственному за организацию обработки ПДн.

2.2.12. Контролировать исполнение пользователями ИСПДн введенного режима безопасности, а так же правильность работы с элементами ИСПДн и средствами защиты.

2.2.13. Контролировать исполнение пользователями правил пользования паролями.

2.2.14. Своевременно анализировать журнал учета событий безопасности, регистрируемых средствами защиты, с целью выявления возможных нарушений и при подозрении на инцидент немедленно докладывать ответственному за организацию обработки ПДн.

2.2.15. Не допускать установку, использование, хранение и размножение в ИСПДн программных средств, не включенных в список разрешенного программного обеспечения.

2.2.16. Не допускать к работе на элементах ИСПДн посторонних лиц.

2.2.17. Осуществлять периодические контрольные проверки правильности функционирования средств защиты ИСПДн.

2.2.18. Оказывать помощь пользователям ИСПДн в части применения средств защиты и консультировать по вопросам введенного режима защиты.

2.2.19. Периодически представлять ответственному за организацию обработки ПДн отчет о состоянии защиты ИСПДн и о нештатных ситуациях на объектах ИСПДн и допущенных пользователями нарушениях установленных требований по защите информации.

2.2.20. В случае отказа работоспособности технических средств и программного обеспечения ИСПДн, в том числе средств защиты принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу

работоспособности.

2.2.21. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

## 3. Права.

3.1. Привлекать к работам, связанным с обеспечением безопасности информации администраторов системных ИСПДн.

3.2. Иметь оборудованное рабочее место.

3.3. Требовать от пользователей ИСПДн соблюдение правил защиты информации в соответствии с организационно – распорядительной документацией по защите персональных данных.

3.4. Требовать от руководства организационного и материального обеспечения для безусловного выполнения своих обязанностей.

## 4. Ответственность.

4.1. На администратора безопасности возлагается персональная ответственность:

4.1.1. за соблюдение режима конфиденциальности информации;

4.1.2. за правильность понимания и полноту выполнения задач, функций, прав и обязанностей, возложенных на него при работе в ИСПДн;

4.1.3. за соблюдение требований локальных актов по вопросам обработки и защиты персональных данных в ИСПДн.

4.1.4. Администратор безопасности несет ответственность, предусмотренную законодательством Российской Федерации.