МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Система менеджмента качества

ИНСТРУКЦИЯ
ПО УПРАВЛЕНИЮ СОБЫТИЯМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Воронеж 2016

1 РАЗРАБОТАНА рабочей группой

2 ОТВЕТСТВЕННЫЙ ИСПОЛНИТЕЛЬ начальник ОИСК Д.В. Макаров

3 УТВЕРЖДЕНА И ВВЕДЕНА В ДЕЙСТВИЕ приказом ректора ВГТУ
от 10.02.2016 № 05–01.18–0

4 ВВОДИТСЯ ВПЕРВЫЕ

1 Общие положения

1.1 Настоящая Инструкция определяет:

– порядок составления и утверждения перечня событий безопасности, подлежащих регистрации и сроки их хранения;

– порядок определения состава и содержания информации о событиях безопасности, подлежащих регистрации;

– порядок сбора, записи и хранения информации о событиях безопасности в течение определённого времени хранения;

– порядок защиты информации о событиях безопасности.

1.2 Настоящая Инструкция разработана на основе нормативных документов

– Федеральный закон от 27.07.2006 № 149–ФЗ «Об информации, информационных технологиях и защите информации».

– Федеральный закон от 27.07.2006 № 152–ФЗ «О персональных данных».

– Приказ ФСТЭК России от 18.02.2013 года №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

– Постановление Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.3 Администратор безопасности и системные администраторы ИСПДн должны быть предупреждены об ответственности за действия, нарушающие требования настоящей инструкции.

1.4 Администратор безопасности и системные администраторы ИСПДн должны быть ознакомлены с настоящей инструкцией до начала работы с ИСПДн под роспись.

1.5 Обязанность ознакомления администратора безопасности и системных администраторов ИСПДн с настоящей инструкцией лежит на ответственном за организацию обработки персональных данных.

2 Перечень событий безопасности подлежащих регистрации

2.1 Перечень событий безопасности, подлежащих регистрации в информационной системе персональных данных (далее – ИСПДн), составляет

администратор безопасности и утверждает ответственный за организацию обработки персональных данных.

2.2 В перечень событий безопасности ИСПДн должны быть включены события безопасности, имеющие отношение к возможности реализации угроз безопасности персональным данным при их обработке в ИСПДн, описанных в модели угроз безопасности персональных данных.

2.3 В перечень событий безопасности ИСПДн должны быть включены события безопасности, регистрируемые в журналах операционной системы технических средств ИСПДн и средств защиты информации (далее – СЗИ), а также организационно-технические события информационной безопасности в инфраструктуре ИСПДн.

2.4 Перечень событий безопасности ИСПДн оформляется в соответствии с приложением 1.

3 Состав и содержание информации о событиях безопасности

3.1 Состав и содержание информации о событиях безопасности ИСПДн, подлежащих регистрации, определяет администратор безопасности и утверждает ответственный за организацию обработки персональных данных.

3.2 Состав и содержание информации по каждому событию, включённому в список регистрации должны идентифицировать источник, время и результат события.

3.3 Форма **перечня состава и содержания информации о событиях безопасности** представлена в приложении 2.

4 Порядок сбора, записи и хранения информации о событиях безопасности

4.1 Настройку журналов регистрации событий информационной безопасности в программном обеспечении ИСПДн и СЗИ осуществляет системный администратор и администратор безопасности ИСПДн каждый в своей части.

4.2 Настройка осуществляется на основе утверждённого перечня событий безопасности, подлежащих регистрации, а также состава и содержания информации о событиях безопасности в соответствии с эксплуатационной документацией на программно–технические средства ИСПДн и средства защиты информации.

4.3 Системные администраторы ИСПДн и администратор безопасности должны **не реже 1 раза в неделю** просматривать журналы регистрации событий безопасности.

4.4 Настройки журналов регистрации событий информационной безопасности должны обеспечивать запись в память технических средств ИСПДн и СЗИ информации о поступающих событиях безопасности без переполнения памяти в течение 1 месяца.

4.5 Информация о событиях безопасности в ИСПДн, не подлежащая автоматической регистрации (нерегистрируемые программно-аппаратные сбои и неисправности, нарушения организационно-правового плана) должна фиксироваться администратором безопасности при её обнаружении в журнале событий безопасности (приложение 3).

5 Защита информации о событиях безопасности

Доступа к файлам отчётов журналов безопасности и настройкам журналов разрешён администратору безопасности, а также ответственным пользователям ИСПДн в соответствии с матрицей доступа.

Приложение 1

Форма перечня событий безопасности, подлежащих регистрации

Уч. № _____

2_____ год

Всего страниц ____

№ п/п	Наименование события ИБ	Обозначение (или код для автоматической регистрации)	Источник	Угроза ИБ	Срок хранения при регистрации

Приложение 2

Форма перечня состава и содержания информации о событиях безопасности

Уч. № _____

2_____ год

Всего страниц ____

№ п/п	Наименование события ИБ	Состав события	Примечание

Приложение 3

Журнал событий безопасности

Уч. № _____

2_____ год.

№ п/п	Наименование события	Описание события	Дата	Подпись