Приложение № 9 к приказу
от 28.06.2019 № 01-09/315
УТВЕРЖДЕНА
приказом генерального директора
КГБОУ ХКЦВР Созвездие
от 28.06.2019 № 01-09/315

# ИНСТРУКЦИЯ

## по управлению конфигурацией

## 1. ВВЕДЕНИЕ

1.1. Настоящая инструкция предназначена для управления конфигурацией информационных систем (далее – ИС), в которых обрабатываются персональные данные (далее – ПДн), в том числе конфигурацией системы защиты информации.

1.2. Настоящая инструкция определяет порядок действий администратора безопасности.

## 2. ПОРЯДОК УПРАВЛЕНИЯ КОНФИГУРАЦИЕЙ

2.1. Базовая конфигурация ИС отображена в документации на ИС.

2.2. Администратор безопасности не реже, чем один раз в год после очередной проверки организует проверку текущей конфигурации ИС и ее системы защиты на соответствие базовой конфигурации. Результат проверки оформляется Актом контроля текущей конфигурации.

2.3. При обнаружении отклонений текущей конфигурации от базовой администратор безопасности организует и контролирует восстановление базовой конфигурации ИС и системы защиты информации. Срок восстановления и мероприятия по восстановлению определяет администратор безопасности.

2.4. Администратору безопасности разрешены решения, направленные на внесение изменений в базовую конфигурацию ИС и систему защиты в случае необходимости.

2.5. Необходимость внесения изменений в базовую конфигурацию ИС и (или) ее систему защиты определяет администратор безопасности:

2.5.1. По результату контроля защищенности информации.

2.5.2. По техническому состоянию технических средств ИС и средств защиты информации.

2.5.3. По актуальности используемых технических средств ИС и средств защиты информации.

2.5.4. По изменениям в технологических процессах обработки информации.

2.5.5. По иным причинам.

2.6. При принятии решения о необходимости внесения изменений в базовую конфигурацию ИС и системы защиты администратор безопасности проводит анализ новых структурно – функциональных характеристик ИС и системы защиты при внесении изменений в базовую конфигурацию.

2.7. На основании:

2.7.1. Анализа результатов изменений в конфигурации.

2.7.2. Анализа действующей модели угроз информационной безопасности.

Администратор безопасности принимает решения:

- либо о внесении изменений в конфигурацию;
- либо об утверждении мероприятий по изменению конфигурации ИС и ее системы защиты генеральным директором.

2.8 Данные о новой конфигурации ИС и (или) ее системы защиты администратор безопасности вносит в документацию с указанием даты внесения изменений.

## 3. НОРМАТИВНЫЕ И ПРАВОВЫЕ ДОКУМЕНТЫ

3.1. Приказ Федеральной службы по техническому и экспортному контролю Российской Федерации от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

3.2. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».