УТВЕРЖДЕНО

Приказом <НАЗВАНИЕ ДОЛЖНОСТИ>
<НАЗВАНИЕ ОРГАНИЗАЦИИ>

<ФИО>

№____ от «___» _____ 20 ___г.

Инструкция управления конфигурацией информационных систем <НАЗВАНИЕ ОРГАНИЗАЦИИ>

Ярославль, 2015

Оглавление

1. Аннотация

Инструкция управления конфигурацией информационных систем (далее – Инструкция) <ПОЛНОЕ НАЗВАНИЕ ОРГАНИЗАЦИИ> (далее – <СОКРАЩЁННОЕ>) определяет общие функции, ответственность, права и обязанности ответственных за управление конфигурацией лиц.

2. Сокращения

Принятое сокращение	Полное наименование
ИБ	Информационная безопасность
ИС	Информационная система
ИТ	Информационные технологии
МЭ	Межсетевой экран
ОС	Операционная система
ТС	Технические средства
ЯО	Ярославская область

3. Термины и определения

Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления.

Информационная безопасность – состояние защищённости интересов Учреждения.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

4. Основания для разработки

Настоящая Инструкция разработана во исполнение требований следующих документов:

- Приказ ФСТЭК России № 17 от 11 февраля 2013 года "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах".
- Методический документ утвержден ФСТЭК России 11 февраля 2014 г. "Меры защиты информации в государственных информационных системах".

5. Общие положения

Базовая конфигурация ИС должна быть задокументирована. Документированию подлежат:

1. Все сетевые подключения ИС к внешним сетям (компьютерам).
2. Все сетевые подключения внешних сетей (компьютеров) к ИС.
3. Параметры настроек ключевых и ТС ИТ-инфраструктуры и средств обеспечения ИБ (маршрутизаторы, коммутаторы, МЭ, ОС и т.п.).
4. Размещение ТС, входящих в состав ИС, с привязкой к границам контролируемой зоны.
5. Состав ТС и ПО, входящих в состав ИС.
6. Состав средств обеспечения ИБ.
7. Топология ИС.

Изменения в конфигурации ИС, способные привести к нарушению конфиденциальности, целостности и доступности защищаемых активов и производственных сервисов, должны

контролироваться и документироваться в журнале регистрации действий по сопровождению ИС и изменению конфигурации (ПРИЛОЖЕНИЕ), в котором необходимо указывать:

1. Дату и время действий по изменению конфигурации.
2. ФИО исполнительного лица.
3. Описание выполненных действий по изменению конфигурации.

Перед внесением изменений в конфигурацию ИС, способных привести к нарушению конфиденциальности, целостности или доступности защищаемых активов и производственных сервисов, должна производиться оценка возможных последствий от таких изменений. Внесение изменений возможно только в случае если такие изменения не приведут к отказу ИС (сервисов ИС) и/или нарушению ИБ.

Существенные изменения в конфигурации ИС, способные привести к нарушению конфиденциальности, целостности или доступности защищаемых активов и производственных сервисов, должны быть санкционированы начальником <НАЗВАНИЕ ОТВЕТСВЕННОГО ПОДРАЗДЕЛЕНИЯ> в письменной форме (ПРИЛОЖЕНИЕ). Несущественные изменения в конфигурации ИС, способные привести к нарушению конфиденциальности, целостности или доступности защищаемых активов и производственных сервисов (<ПРИМЕРЫ>) санкционируются системным администратором.

5.1. Документирование сведений о сетевых подключениях

Все сетевые подключения ИС к внешним сетям документируются, а также должны подвергаться мониторингу и контролю. Для каждого сетевого подключения к внешним сетям должно быть определено:

1. Наименование сети, к которой осуществляется подключение.
2. Состав серверов и рабочих станций, которые будут подключены к внешним сетям.
3. Предполагаемые к использованию сервисы внешних сетей.
4. Факт передачи конфиденциальной информации с указанием её состава.
5. Факт хранения конфиденциальной информации на серверах и рабочих станциях, подключаемых к внешним сетям.
6. Перечень пользователей, которым предоставлено право использовать сервисы внешних сетей.
7. Режим подключения ИС к внешним сетям (постоянный, временный).

Подключения должны быть санкционированы начальником <НАЗВАНИЕ ОТВЕТСВЕННОГО ПОДРАЗДЕЛЕНИЯ>. Доступ к внешним сетям должен быть разрешён только тем сотрудникам < НАЗВАНИЕ ОРГАНИЗАЦИИ>, которым он необходим для выполнения задач, возложенных на них в соответствии с должностными обязанностями. Предоставление пользователям полномочий на доступ к сервисам внешних сетей должно осуществляться с учётом принципа минимальной необходимости.

Все сетевые подключения внешних сетей (компьютеров) к ИС документируются, а также должны подвергаться мониторингу и контролю. Для каждого удалённого подключения внешних сетей (компьютеров) к ИС должно быть определено:

1. Наименование внешней сети (компьютера), подключаемой к ИС.
2. Вид удалённого доступа (удалённый доступ к сервису, удалённое администрирование и/или работа в режиме удалённого узла сети).
3. Предполагаемые к использованию внешними пользователями сервисы и/или активы ИС.
4. Факт передачи конфиденциальной информации с указанием её состава.

5. Перечень пользователей < НАЗВАНИЕ ОРГАНИЗАЦИИ> и\или сторонних организаций, которым предоставлено право удалённого доступа к ИС.

Подключения должны быть санкционированы начальником <НАЗВАНИЕ ОТВЕТСВЕННОГО ПОДРАЗДЕЛЕНИЯ>. Удалённый доступ должен быть разрешён только тем сотрудникам < НАЗВАНИЕ ОРГАНИЗАЦИИ> и\или сотрудникам сторонних организаций, которым он необходим для выполнения задач, возложенных на них в соответствии с должностными обязанностями.

Начальные требования к параметрам защиты МЭ при осуществлении межсетевого взаимодействия должны быть зафиксированы в проектной документации на систему защиты информации ИС. Текущие параметры настройки устанавливаемых МЭ должны быть закреплены в рабочей документации на эти МЭ. Пример документирования настроек МЭ приведён в приложении (ПРИЛОЖЕНИЕ).

5.2. Документирование программного обеспечения

Инвентаризация программного обеспечения проводится на всех без исключения компьютерах, входящих в состав ИС. Инвентаризации подлежат все без исключения экземпляры программного обеспечения, включая как устанавливаемые стандартными средствами и видимые в разделе «Установка и удаление программ» Панели Управления ОС Windows, так и экземпляры дистрибутивов и рабочих копий программ, находящихся на всех без исключения перезаписываемых носителях, подключённых к компьютеру, включая жёсткие диски, постоянно используемые с данным компьютером карты памяти, оптические перезаписываемые диски и т.п.

На каждый компьютер составляется электронная инвентаризационная карточка по форме «Инвентаризационная карточка» (ПРИЛОЖЕНИЕ).

Перечень разрешённого к использованию в ИС ПО должен быть документально закреплён (ПРИЛОЖЕНИЕ). В перечне должны быть указаны:

1. Наименование.
2. Производитель.
3. Версия.
4. Платформа.
5. Число инсталляций.
6. Информация о лицензиях, находящихся в законном наличии и/или распоряжении.

Отдельной перепроверке и инвентаризации подлежат следующие активы:

1. Документы на приобретение ПО.
2. Носители.
3. Руководства пользователя.
4. Сопроводительные материалы.

Результаты инвентаризации активов вносятся в реестр по форме «Реестр сопроводительной документации и сопутствующих активов программного обеспечения» (ПРИЛОЖЕНИЕ).

5.3. Документирование состав технических средств

Инвентаризация технических средств проводится в отношении всех без исключения компьютеров, серверов, и сетевого оборудования, входящего в состав ИС.

На каждый ТС, входящее в состав ИС составляется электронная инвентаризационная карточка по форме «Инвентаризационная карточка» (ПРИЛОЖЕНИЕ).

6. Обязанности

<НАЗВАНИЕ ОТВЕТСВЕННОГО ПОДРАЗДЕЛЕНИЯ> осуществляет мониторинг изменений конфигурации ИС с целью подтверждения защищённости ИС после внесения изменений в конфигурацию ИС и анализа их эффективности.

Пользователям ИС не допускается вносить изменения в конфигурацию ИС самостоятельно (устанавливать новое, удалять или изменять настройки имеющегося ПО, устанавливать новые ТС, отключать средства обеспечения ИБ и т.п.).

Начальник <НАЗВАНИЕ ОТВЕТСВЕННОГО ПОДРАЗДЕЛЕНИЯ> :

- Осуществляет общее методическое руководство деятельностью по упарвлению конфигурациями ИС.
- Санкционирует существенные изменения конфигурации ИС.
- Информирует руководство < НАЗВАНИЕ ОРГАНИЗАЦИИ> о состоянии дел в области обеспечения ИБ.
- Осуществляет контроль за соблюдением положений настоящей Инструкции.

Администратор ИБ:

- Проводит мониторинг изменений конфигурации ИС.

Сотрудники <НАЗВАНИЕ ОТВЕТСВЕННОГО ПОДРАЗДЕЛЕНИЯ>:

- Документируют базовую конфигурацию ИС.
- Документируют изменения в конфигурации ИС.
- Осуществляют санкционированные изменения в конфигурации ИС.

7. Ответственность

Каждый сотрудник, имеющий доступ в ИС несёт персональную ответственность за обеспечение ИБ в соответствии с требованиями настоящей Инструкции.

Лица, нарушившие требования безопасности, изложенные в настоящей Инструкции могут быть привлечены к дисциплинарной или административной ответственности в соответствии с действующим законодательством Российской Федерации.

8. Контроль и пересмотр

<НАЗВАНИЕ ОТВЕТСВЕННОГО ПОДРАЗДЕЛЕНИЯ> по мере необходимости, но не реже чем в пять лет, пересматривает настоящую Инструкцию. Изменения и дополнения вносятся по инициативе <НАЗВАНИЕ ОТВЕТСВЕННОГО ПОДРАЗДЕЛЕНИЯ> или <Директора> и утверждаются <Директором>.

Все изменения, внесённые в настоящую Инструкцию должны учитываться в листе «История изменений».

9. История изменений

Версия	Дата утверждения	Изменения	Кто внёс изменения

Приложение 1. Журнал регистрации изменений конфигурации

ЖУРНАЛ
учёта изменений в конфигурации сервера администрирования антивирусной защиты Kaspersky Security Center

Начат «____» _____ 20___ г.
Должность _____

_____
ФИО должностного лица _____

_____

Окончен «____» _____ 20___ г.
Должность _____

_____
ФИО должностного лица _____

_____

№ п/п	№ заявки на внесение изменений	ФИО ответственного лица, внёсшего изменения	Подпись	Дата внесения изменений	№ акта	Примечание

Приложение 2. Форма запроса на изменение

Заявка № _____

на внесение изменений в конфигурацию ИС (проекта)

1. Прошу внести изменение в конфигурацию информационной системы

Автор запроса (Ф.И.О. сотрудника): _____
Должность: _____
Наименование структурного подразделения: _____

Название ИС _____
Краткое описание предлагаемого изменения _____
Обоснование необходимости внесения изменения _____

_____
(должность)

_____ _____ «____» _____ ____г.
(Ф.И.О.) *(Подпись)* *(Дата)*

2. Возможность внести изменение в конфигурацию информационной системы в указанных целях согласую

_____
(должность)

_____ _____ «____» _____ ____г.
(Ф.И.О.) *(Подпись)* *(Дата)*

3. Возможность внести изменение в конфигурацию информационной системы в указанных целях подтверждаю

_____
(должность)

_____ _____ «____» _____ ____г.
(Ф.И.О.) *(Подпись)* *(Дата)*

4. Отметка исполнителя

Выполненные действия _____

_____
(должность)

_____ _____ «____» _____ ____г.
(Ф.И.О.) *(Подпись)* *(Дата)*

Приложение 3. Пример документирования настроек МЭ

№	Сервер	Сервис	Политика		Примечание
			Исходящие	Входящие	
1	Почтовый сервер <IP>	SMTP <порт>	да	да	
2					
3					
4					

Примечание: Политика по умолчанию запрещает любые соединения, кроме описанных в таблице.

Приложение 4. Инвентаризационная карточка компьютера

Инвентаризационная карточка

Инвентаризацию провёл:

_____
(должность)

_____ _____ «____» _____ _____г.
(Ф.И.О.) *(Подпись)* *(Дата)*

Характеристики:

Тип оборудования (стационарный, переносной, сервер, др. оборудование): _____
Производитель: _____
Модель: _____

Состав ПО (при наличии):

№	Наименование	Производитель	Версия	Информация о лицензиях
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				

Состав ТС:

№	Наименование	Производитель	Версия	Информация о лицензиях
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				

Приложение 5. Перечень разрешённого к использованию программного обеспечения

Перечень разрешённого к использованию программного обеспечения

Перечень составил:

_____
(должность)

_____ _____ «____» _____ _____г.
(Ф.И.О.) *(Подпись)* *(Дата)*

Перечень ПО:

№	Наименование	Производитель	Версия	Число инсталляций	Информация о лицензиях
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					

Приложение 6. Реестр сопроводительной документации

Реестр сопроводительной документации

Реестр составил:

_____
(должность)

_____ _____ «____» _____ _____г.
(Ф.И.О.) *(Подпись)* *(Дата)*

Документы, доказывающие законность владения:

№	ПО/ИС	Накладная	Счёт-фактура	Другие
1				
2				
3				
4				
5				

Реестр сопроводительной документации:

№	ПО/ИС	Документ	Комментарий
6			
7			
8			
9			
10			