УТВЕРЖДЕНО
приказом директора МАУ ДО
«Детско-юношеский центр»
№ 23 от 14 января 2019 года

Инструкция
по модификации технических и программных средств информационной системы в муниципальном автономном учреждении дополнительного образования «Детско-юношеский центр»

1. Общие положения

1.1. Настоящей инструкцией регламентируется взаимодействие подразделений и сотрудников Муниципального автономного учреждения дополнительного образования «Детско=юношеский центр» (далее – Организация) при проведении модификаций программного обеспечения, технического обслуживания средств вычислительной техники, а так же при возникновении нештатных ситуаций в работе защиты информационной системы «Сетевой Город. Образование» и Е-услуги. Образование» (далее – информационная система, ИС).

1.2. Право внесения изменений в конфигурацию аппаратно-программных средств защищенных рабочих станций и серверов ИС предоставляется системному администратору ИС.

1.3. Изменение конфигурации аппаратно-программных средств защищенных рабочих станций и серверов кем-либо, кроме системного администратора, запрещено.

1.4. Установка, изменение (обновление) и удаление системных и прикладных программных средств производится уполномоченными сотрудниками. Если АРМ или сервер относится к защищаемым рабочим станциям, то установка, снятие, и внесение необходимых изменений в настройки средств защиты осуществляется с участием администратора безопасности информации (далее – АБИ).

1.5. Основанием для внесения изменений в программное обеспечение и состав технических средств является заявка (Приложение № 1). В заявке указываются следующие виды изменений в составе технических и программных средств:

- добавление устройства (узла, блока);
- замена устройства (узла, блока);

– изъятие устройства (узла, блока);

– установка (развертывание) программных средств, необходимых для решения определенной задачи, добавление возможности, решения новой задачи;

– обновление (замена) программных средств;

– удаление программных средств.

1.6. Администратор безопасности информации рассматривает заявку, определяет возможность внесения изменений и вносит изменения в состав аппаратных средств и программного обеспечения.

1.7. Установка или обновление подсистем ИС должны проводиться в строгом соответствии с технологией проведения модификаций программных комплексов данных подсистем.

1.8. Установка и обновление общего программного обеспечения (далее – ПО) (системного, тестового и т.п.) на рабочие станции и сервера производится с оригинальных лицензионных дистрибутивных носителей (дискет, компакт дисков и т.п.), полученных установленным порядком, а прикладного ПО – с эталонных копий программных средств, полученных из сетевого архива эталонных дистрибутивов программ. При необходимости (в случае установки части компонент на дисках сетевых серверов) к работам привлекаются администраторы сети (серверов) и администраторы баз данных.

1.9. Все добавляемые программные и аппаратные компоненты должны быть предварительно установленным порядком проверены на работоспособность, а также отсутствие опасных функций.

1.10.После установки (обновления) программного обеспечения администратор безопасности информации должен произвести настройку средств управления доступом к компонентам данной задачи (программного средства) в соответствии с ее (его) формуляром и совместно с ответственным пользователем АРМ должен проверить работоспособность ПО и правильность настройки средств защиты.

1.11.При изъятии АРМ из состава рабочих станций подразделения ее передача на склад, в ремонт или в другое подразделение для решения иных задач осуществляется только после того, как администратор безопасности информации снимет с данной ПЭВМ средства защиты и предпримет необходимые меры для затирания защищаемой информации, которая хранилась на дисках компьютера. Факт уничтожения данных, находившихся на диске компьютера, оформляется актом за подписью ответственного за информационную безопасность в подразделении.

1.12.При модификации технических и программных средств, входящих в состав систем, аттестованных по требованиям безопасности информации необходимо уведомить об осуществлённых изменениях организацию, проводившую аттестацию, которая принимает решение о необходимости проведения контроля эффективности аттестованного объекта информатизации.

1.13.Все изменения конфигурации технических и программных средств АРМ и серверов, входящих в аттестованные по требованиям безопасности информации, отражаются в Техническом паспорте объекта информатизации.

1.14.Запрещается изменение состава (в том числе ввод новых) программных средств, осуществляющих обработку защищаемой информации на объектах информатизации, аттестованных по требованиям безопасности информации.

2. Экстренная модификация (обстоятельства непреодолимой силы)

2.1. В исключительных случаях (сбой ПО, не позволяющий продолжить работу), требующих безотлагательного изменения ПО, допускается корректировка программ непосредственно на рабочей станции. В данной ситуации сотрудник Организации ставит в известность администратора безопасности информации о необходимости такого изменения. При необходимости проводится изменение ПО загрузочного раздела сервера. Если это необходимо, администратор безопасности информации вносит необходимые корректировки в настройки системы контроля целостности ПО АРМ и сервера.

2.2. Факт модификации ПО и корректировки настроек системы защиты фиксируется в «Журнале учета мероприятий по обеспечению информационной безопасности».

3. Порядок проверки работоспособности системы защиты после установки (обновления) программных средств и внесения изменений в списки пользователей

3.1. После установки (обновления) программных средств или внесения изменений в списки пользователей системы администратор безопасности информации обязан проверить работоспособность технических средств и правильность настройки установленных средств защиты.

3.2. При установке нового (обновлении существующего) программного средства администратор ИС обязан:

- установить права доступа пользователей системы к файлам программного средства таким образом, как это указано в формуляре на

программное средство (задачу);

- программными средствами подсчитать контрольные суммы файлов программных средств (при наличии указаний в формуляре);
- если для пользователя, использующего установленное программное средство, установлен режим замкнутой программной среды, необходимо программными средствами добавить в список разрешенных ему для запуска программ исполняемые модули данного пакета.

После осуществления данных действий необходимо проверить корректность функционирования системы защиты, для чего требуется произвести следующие действия:

- для каждого пользователя, для которого установлен режим замкнутой программной среды, требуется проверить работоспособность установленного программного средства и сохранение режима замкнутой программной среды;
- в режиме обычного пользователя необходимо проверить возможность удаления вновь установленных (обновленных) файлов.

Приложение № 1
к Инструкции по модификации
технических и программных средств

Администратору безопасности
информации информационной системы
персональных данных

_____
(ФИО)

От _____
(Фамилия)

_____
(Имя, Отчество)

_____
(наименование должности)

_____
(структурное подразделение)

заявление.

Прошу Вас внести изменения в конфигурацию

_____
(наименование и место установки рабочей станции / сервера)

в соответствии с прилагаемой таблицей.

«_____» _____ 20__ г. _____
(подпись)

СОГЛАСОВАНО
Руководитель структурного подразделения:

_____	_____	_____
(ФИО)	(подпись)	(дата)

ОТМЕТКА О ВЫПОЛНЕНИИ
Системный администратор

_____	_____	_____
(ФИО)	(подпись)	(дата)

Таблица 1 – Перечень необходимых изменений конфигурации рабочей станции / сервера

№ п/п	Наименование информационного ресурса/сервиса	Изменение	Обоснование
1.			
2.			
3.			
4.			
5.			