**УТВЕРЖДАЮ**
Директор

_____М.В.Облицов

# ИНСТРУКЦИЯ
# ПО УСТАНОВКЕ, МОДИФИКАЦИИ И ТЕХНИЧЕСКОМУ ОБСЛУЖИВАНИЮ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И АППАРАТНЫХ СРЕДСТВ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ООО «АГЕНТ»

Томск 2011

СОГЛАСОВАНО:

| | | |
|---|---|---|
| Заместитель директора | _____ (подпись) | _____ (дата) |
| Заместитель директора по экономическим вопросам | _____ (подпись) | _____ (дата) |

Настоящей инструкцией регламентируется взаимодействие подразделений ООО "Агент" (далее – Учреждение) по обеспечению безопасности информации при проведении модификаций программного обеспечения, технического обслуживания средств вычислительной техники и при возникновении нештатных ситуаций в работе автоматизированной системы Учреждения.

Все изменения конфигурации технических и программных средств защищенных рабочих станций (РС) и серверов Учреждения должны производиться только на основании заявок начальников структурных подразделений либо заявок начальника отдела информационных технологий (ОИТ), согласованных с ответственным за обеспечение информационной безопасности.

Право внесения изменений в конфигурацию аппаратно-программных средств защищенных рабочих станций и серверов Учреждения предоставляется:

- в отношении системных и прикладных программных средств, а также в отношении аппаратных средств - уполномоченным сотрудникам ОИТ;
- в отношении программно-аппаратных средств защиты - уполномоченным сотрудникам ОИТ и ответственному за обеспечение информационной безопасности;
- в отношении программно-аппаратных средств телекоммуникации - уполномоченным сотрудникам ОИТ.

Изменение конфигурации аппаратно-программных средств защищенных рабочих станций и серверов кем-либо, кроме уполномоченных сотрудников перечисленных подразделений, **ЗАПРЕЩЕНО**.

Процедура внесения изменений в конфигурацию аппаратных и программных средств защищенных серверов и РС системы инициируется заявкой начальника данного подразделения либо заявкой начальника ОИТ. Формы заявок приведены ниже.

Заявка руководителя подразделения органа Учреждения, в котором требуется произвести изменения конфигурации РС, оформляется на имя начальника ОИТ. Производственная необходимость проведения указанных в заявке изменений подтверждается подписью ответственного за обеспечение информационной безопасности Учреждения.

Заявка руководителя ОИТ, который отвечает за плановое проведение изменений (обновлений версий) ПО, оформляется на имя руководителя структурного подразделения (подразделений), использующего (использующих) подсистему АС, требующую модификации. Производственная необходимость проведения указанных в заявке изменений подтверждается подписью ответственного за обеспечение информационной безопасности Учреждения.

В заявках могут указываться следующие виды необходимых изменений в составе аппаратных и программных средств РС и серверов подразделения:

- установка в подразделении новой ПЭВМ (развертывание новой РС или сервера);
- замена ПЭВМ (РС или сервера подразделения);
- изъятие ПЭВМ (РС или сервера подразделения);
- добавление устройства (узла, блока) в состав конкретной РС или сервера подразделения;
- замена устройства (узла, блока) в составе конкретной РС или сервера подразделения;
- изъятие устройства (узла, блока) из состава конкретной РС или сервера;

- установка (развертывание) на конкретной РС или сервера программных средств, необходимых для решения определенной задачи (добавление возможности решения данной задачи на данной РС или сервере);
- обновление (замена) на конкретной РС или сервере программных средств, необходимых для решения определенной задачи (обновление версий используемых для решения определенной задачи программ);
- удаление с конкретной РС или сервера программных средств, использовавшихся для решения определенной задачи (исключение возможности решения данной задачи на данной РС).

В заявке указываются условные наименования развернутых РС и серверов в соответствии с их формулярами. В случае развертывания новой РС ее наименование в заявке указывать не требуется (оно устанавливается позднее при заполнении формуляра новой РС).

Заключение о технической возможности осуществления затребованных изменений выдается специалистами ОИТ.

Заключение о возможности совмещения решения новых задач (обработки информации) на указанных в заявке РС или серверах в соответствии с требованиями по безопасности выдается ответственным за обеспечение информационной безопасности Учреждения, которому заявка передается на согласование (одновременно с этим производится определение новых категорий защищенности указанных РС или серверов).

После чего заявка передается в ОИТ для непосредственного исполнения работ по внесению изменений в конфигурацию РС или серверов Учреждения.

Руководитель подразделения допускает уполномоченных исполнителей к внесению изменений в состав аппаратных средств и программного обеспечения только по предъявлении последними утвержденной заявки на осуществление данных изменений.

Установка, изменение (обновление) и удаление системных и прикладных программных средств производится уполномоченными сотрудниками ОИТ. Если РС или сервер относится к защищаемым рабочим станциям, то установка, снятие, и внесение необходимых изменений в настройки средств защиты от НСД и средств контроля целостности файлов на РС производятся в присутствии ответственного за информационную безопасность, руководителя подразделения и пользователя данной РС.

Подготовка модификаций программного обеспечения защищенных серверов и рабочих станций, тестирование, стендовые испытания и передача исходных текстов, документации и дистрибутивных носителей программ в архив эталонных дистрибутивов Учреждения и другие необходимые действия производятся ОИТ согласно утвержденным инструкциям.

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

Модификация ПО на сервере осуществляется уполномоченными сотрудниками ОИТ обязательно в присутствии ответственного за обеспечение информационной безопасности Учреждения. После установки модифицированных модулей на сервер ответственный за обеспечение информационной безопасности в присутствии сотрудников ОИТ устанавливает защиту целостности модулей на сервере (производит пересчет контрольных сумм эталонов модулей на файл-сервере с помощью средств Secret Net). После проведения модификации ПО на рабочих станциях сотрудник ОИТ проводит антивирусный контроль.

Установка и обновление общего 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. При необходимости (в случае установки части компонент на дисках сетевых серверов) к работам привлекаются администраторы сети (серверов) и администраторы баз данных.

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

После установки (обновления) ПО ответственный за обеспечение информационной безопасности должен произвести настройку средств управления доступом к компонентам данной задачи (программного средства) в соответствии с ее (его) формуляром и совместно с сотрудником ОИТ и ответственным пользователем РС должен проверить работоспособность ПО и правильность настройки средств защиты в соответствии с “Порядком проверки работоспособности системы защиты после установки (обновления) программных средств РС”.

После завершения работ по внесению изменений в состав аппаратных средств защищенной РС ее системный блок должен закрываться сотрудником ОИТ на ключ (при наличии штатных механических замков) и опечатываться (пломбироваться, защищаться специальной наклейкой) ответственным за обеспечение информационной безопасности Учреждения.

Уполномоченные исполнители работ от ОИТ должны произвести соответствующую запись в «Журнале учета нештатных ситуаций, фактов вскрытия и опечатывания ПЭВМ, выполнения профилактических работ, установки и модификации аппаратных и программных средств РС подразделения». Делают отметку о выполнении (на обратной стороне заявки) и передают исполненную заявку ответственному за информационную безопасность в подразделении для хранения вместе с формуляром данной РС (сервера).

Формат записей в Журнал учета нештатных ситуаций, фактов вскрытия и опечатывания ПЭВМ, выполнения профилактических работ, установки и модификации аппаратных и программных средств РС подразделения:

| N п/п | Дата | Краткое описание выполненной работы (нештатной ситуации) | ФИО исполнителей и их подписи | ФИО ответственного пользователя РС, подпись | Подпись ответственного за информационную безопасность подразделения | Примечание (ссылка на заявку) |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| | | | | | | |
| | | | | | | |

При изъятии РС из состава рабочих станций подразделения ее передача на склад, в ремонт или в другое подразделение для решения иных задач осуществляется только после того, как ответственный за обеспечение информационной безопасности Учреждения 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. Форма Акта приведена ниже.

Допуск новых пользователей к решению задач с использованием вновь развернутого ПО (либо изменение их полномочий доступа) осуществляется согласно «Инструкции по

внесению изменений в списки пользователей системы и наделению пользователей полномочиями доступа к ресурсам Учреждения».

Оригиналы заявок (документов), на основании которых производились изменения в составе технических или программных средств РС с отметками о внесении изменений в состав аппаратно-программных средств должны храниться вместе с оригиналами формуляров РС и «Журналом учета…» в подразделении (у ответственного за информационную безопасность или руководителя подразделения). Копии заявок и актов могут храниться в ОИТ. Они могут использоваться:

- для восстановления конфигурации РС после аварий;
- для контроля правомерности установки на конкретной РС средств для решения соответствующих задач при разборе конфликтных ситуаций;
- для проверки правильности установки и настройки средств защиты РС.

## ЭКСТРЕННАЯ МОДИФИКАЦИЯ (ОБСТОЯТЕЛЬСТВА ФОРС-МАЖОР)

В исключительных случаях (сбой ПО, не позволяющий продолжить работу), требующих безотлагательного изменения ПО, допускается корректировка программ непосредственно на рабочей станции. В данной ситуации сотрудник ОИТ ставит в известность руководство ОРГАНИЗАЦИИ и ответственного за обеспечение информационной безопасности о необходимости такого изменения. Факт внесения изменений в ПО РС фиксируется актом за подписями ответственного за информационную безопасность в подразделении и пользователя данной РС и сотрудников ОИТ. В акте указывается причина модификации, перечисляются файлы, подвергшиеся изменению, и указывается лицо(а), проводившее изменения. При необходимости проводится изменение ПО загрузочного раздела сервера. Если это необходимо, сотрудник службы ОБИ вносит необходимые корректировки в настройки системы контроля целостности ПО РС и сервера. Факт модификации ПО и корректировки настроек системы защиты фиксируется в «Журнале учета нештатных ситуаций...» того подразделения, в котором установлена РС (сервер).

В течение следующего дня после составления акта руководством ОИТ и ответственного за обеспечение информационной безопасности при участии сотрудников подразделения выясняются причины и состав проведенных экстренных изменений, и принимается решение о необходимости подготовки исправительной модификации ПО или восстановления ПО РС (сервера) с эталонной копии. Необходимость участия в разбирательстве сотрудника подразделения определяется руководством. Результат разбирательства оформляется в виде согласованного решения и хранится в ОИТ, копии передаются ответственному за обеспечение информационной безопасности.

Начальнику отдела информационных технологий

(резолюция ответственного за обеспечение
информационной безопасности)
“ _–_ “ _____ 20 __ года

# ЗАЯВКА
## на внесение изменений в состав аппаратно-программных средств АС

Прошу произвести следующие изменения конфигурации аппаратно - программных средств автоматизированной подсистемы

_____ -

(наименование подразделения)

развернуть новую рабочую станцию и установить на (обновить на / снять с) нее _____ компоненты, необходимые для решения следующих задач:

_____

(наименование задач)

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Начальник _____

(наименование подразделения заказчика)

«___–» _____ 20__ г. _____ _____

(подпись) (фамилия и инициалы)

Начальнику отдела информационных технологий

(резолюция ответственного за обеспечение
информационной безопасности)
“ ___ “ _____ 20 ___ года

# ЗАЯВКА
## на внесение изменений в состав аппаратно-программных средств АС

В связи с необходимостью

_____

(обоснование причины внесения изменений)

_____

_____

прошу допустить установленным порядком сотрудников ОИТ:

_____

(фамилии исполнителей)

_____

для выполнения необходимых работ в

_____

(наименование подразделения)

по установке рабочей станции (обновлению / снятию с РС _____ компонентов),
необходимых для решения следующих задач:

_____

(наименование задач)

_____
_____
_____
_____
_____
_____
_____
_____

Начальник ОИТ

«____» _____ 20___ г. _____ _____
(подпись) (фамилия и инициалы)

*Обратная сторона заявки*

## Отметка о выполнении

### (о внесении изменений в состав аппаратно-программных средств АС)

В соответствии с “Инструкцией по установке, модификации и техническому обслуживанию программного обеспечения и технических средств РС АС ОГБУЗ «ОПЦ»” рабочей группой в составе:

от отдела информационных технологий

_____

от ответственного за обеспечение информационной безопасности

_____

от подразделения (отдела)

_____

указанные в заявке изменения внесены (не внесены по следующей причине):

_____

краткое пояснение причины

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____Изменения в формуляр РС (ссылка на данную заявку) внесены.

От отдела _____ От ОИТ

_____ _____

(подпись, фамилия) (подпись, фамилия)

«____» _____ 20___ г.

Ответственный за обеспечение

информационной безопасности

_____

(подпись, фамилия)

«____» _____ 20___ г.

# АКТ

## о затирании остаточной информации, хранившейся на диске компьютера

Все файлы, содержащие подлежащую защите информацию, находившиеся на НЖМД №_____, передаваемого

_____

(с какой целью)

_____

(Кому: должность, Ф.И.О.)

---

системного блока ПЭВМ марки _____ серийный №_____

уничтожены (затерты) посредством программы

_____.

Начальник отдела информационных технологий

_____

(Ф.И.О.)

_____ _____

(Подпись) (Дата)

Ответственный за обеспечение информационной безопасности Учреждения

_____

(Ф.И.О.)

_____ _____

(Подпись) (Дата)

## ПОРЯДОК ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ И РЕМОНТА ТЕХНИЧЕСКИХ СРЕДСТВ РС АС ОРГАНИЗАЦИИ

Техническое обслуживание и ремонтные работы на технических средствах ПЭВМ РС должны осуществляться только уполномоченными сотрудниками ОИТ, назначенными ответственными за их обслуживание (сопровождение). Их вызов осуществляется сотрудниками подразделения, эксплуатирующего РС, при возникновении нештатных ситуаций.

К нештатным ситуациям относятся:

- выход из строя или неустойчивое функционирование узлов ПЭВМ или периферийных устройств (например, дисковода, принтера) РС;
- выход из строя системы электроснабжения РС.

Техническое обслуживание и регламентные работы могут проводиться в плановом порядке. В этом случае работы проводятся на основании утвержденных руководством и согласованных с ответственным за обеспечение информационной безопасности.

Ответственность за соблюдение требований по обеспечению безопасности информации при проведении технического обслуживания и ремонтных работ на ПЭВМ возлагается ответственного за информационную безопасность (либо руководителя) подразделения.

Уполномоченные сотрудники ОИТ имеют право доступа к РС для разбора нештатных ситуаций без участия ответственного за информационную безопасность при обнаружении сбоев в их работе только для тестирования ПЭВМ с использованием установленных на РС (в сети) тестовых средств.

О факте выполнения данных работ ответственный за информационную безопасность подразделения делает соответствующую отметку в «Журнале учета…» с указанием признаков проявления ситуации и содержания выполненных работ по ее устранению.

При необходимости осуществления изменений аппаратно-программной конфигурации РС соответствующие работы выполняются с соблюдением требований «Инструкция по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств автоматизированной системы Учреждения».

# ПОРЯДОК ПРОВЕРКИ РАБОТОСПОСОБНОСТИ СИСТЕМЫ ЗАЩИТЫ ПОСЛЕ УСТАНОВКИ (ОБНОВЛЕНИЯ) ПРОГРАММНЫХ СРЕДСТВ АС И ВНЕСЕНИЯ ИЗМЕНЕНИЙ В СПИСКИ ПОЛЬЗОВАТЕЛЕЙ

После установки (обновления) программных средств РС или внесения изменений в списки пользователей системы ответственный за информационную безопасность обязан проверить работоспособность РС и правильность настройки средств защиты, установленных на компьютере.

При установке нового (обновлении существующего) программного средства ответственный за информационную безопасность обязан:

- установить права доступа пользователей системы к файлам программного средства таким образом, как это указано в формуляре на программное средство (задачу);
- средствами системы Secret Net подсчитать контрольные суммы файлов программных средств (при наличии указаний в формуляре);
- если для пользователя, использующего установленное программное средство, установлен режим замкнутой программной среды, необходимо средствами системы Secret Net 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 РС, 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.