|  |
| --- |
| Приложение 3 к Положению об обеспечении безопасности общедоступной информации в информационных системах комитета по финансам, налоговой и кредитной политике города Барнаула |

ПОРЯДОК

технического обслуживания, ремонта, модернизации технических средств, входящих в состав информационных систем комитета по финансам, налоговой и кредитной политике города Барнаула

# Перечень используемых определений, обозначений и сокращений

АИБ – администратор информационной безопасности.

АРМ – автоматизированное рабочее место.

АС – автоматизированная система.

АСО – активное сетевое оборудование.

АЭД – архив эталонных дистрибутивов.

ИБ – информационная безопасность.

ИС – информационная система.

ИТ (IT) – информационные технологии.

КИ – конфиденциальная информация.

КИС – корпоративная информационная система.

ЛВС – локальная вычислительная сеть.

НЖМД – накопитель на жёстких магнитных дисках.

НСД – несанкционированный доступ.

ПК – персональный компьютер.

ПО – программное обеспечение.

ПЭВМ – персональная электронная вычислительная машина.

СБ – служба безопасности.

СВТ – средства вычислительной техники.

СЗИ – средства защиты информации.

СУБД – система управления базами данных.

ФСТЭК – Федеральная служба по техническому и экспортному контролю.

ЭД– эксплуатационная документация.

Администратор информационной безопасности – специалист отдела внедрения автоматизированных систем финансовых расчетов, осуществляющий контроль за обеспечением защиты информации в ИС, а также осуществляющий организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления НСД к защищаемой информации.

1. Общие положения
   1. Настоящий Порядок регламентирует взаимодействие сотрудников комитета по финансам, налоговой и кредитной политике города Барнаула по вопросам обеспечения безопасности в информационных системах общего пользования, государственных информационных системах, муниципальных информационных системах, информационных системах персональных данных, информационных системах, содержащих другие виды конфиденциальной информации, за исключением систем, содержащих сведения, составляющие государственную тайну, и систем, относящихся к ключевым системах информационной инфраструктуры (далее по тексту – ИС, защищаемые информационные ресурсы) при проведении модификаций ПО, технического обслуживания СВТ и при возникновении нештатных ситуаций в работе ИС.
   2. Под техническим обслуживанием (далее – ТО) в данном документе понимается комплекс операций по поддержанию работоспособности или исправности оборудования при использовании по назначению, ожидании, хранении и транспортировке.
   3. ТО СВТ направлено на обеспечение постоянной готовности оборудования к использованию Пользователем по прямому назначению, рациональной загрузки Пользователем оборудования и предотвращение преждевременного выхода его из строя в связи с нарушениями Пользователем правил технической эксплуатации.
   4. Обновление ПО, в результате которого в самом ПО не возникает значительных изменений (новые модули, изменяется версия программного продукта и т.п.), в данном документе не рассматривается как модификация.
2. Виды технического обслуживания
   1. В комитете по финансам, налоговой и кредитной политике города Барнаула проводится техническое обслуживание следующих видов:

* плановое – производимое не менее 1 раз в год, если иное не указано в сопроводительной документации на СВТ;
* внеочередное ТО СВТ, производимое по Заявке на внесение изменений в состав аппаратно-программных средств ИС (Приложение 1) (далее – заявка) пользователя при сбоях или отказах оборудования.

1. Организация работ
   1. ТО СВТ проводится только на оборудовании, находящегося на балансе комитета по финансам, налоговой и кредитной политике города Барнаула.
   2. План ТО СВТ (Приложение 2) утверждается после согласования председателем комитета по финансам, налоговой и кредитной политике города Барнаула и предоставляется пользователю не менее чем за неделю до начала производства работ.
   3. Факт проведения ТО СВТ фиксируется в журнале проверки исправности и технического обслуживания (Приложение 3).
   4. Если для выполнения внеочередного ТО СВТ необходимо произвести работы, входящие в плановое ТО СВТ, то плановое ТО считается в данный период выполненным, и дата следующего планового ТО СВТ сдвигается на соответствующий периодический срок.
   5. Внеочередное ТО СВТ производится на основании заявки, которая заверяется подписями руководителя структурного подразделения (начальника отдела) и пользователя. В заявке обязательно указывается текущая дата, тип или модель средства вычислительной техники, серийный (или заводской) номер, местонахождение оборудования, характер и обстоятельства возникновения возможной неисправности. Учет заявок фиксируются в журнале проверки исправности и технического обслуживания.
   6. Заключение о технической возможности осуществления затребованных изменений выдается системным администратором (на основании формуляров соответствующих АРМ или серверов).
   7. Заключение о возможности совмещения решения новых задач (обработки информации) на указанных в заявке АРМ или серверах в соответствии с требованиями по безопасности выдается АИБом, которому заявка передается на согласование (одновременно с этим производится определение новых категорий защищенности указанных АРМ или серверов).
   8. После этого заявка передается системному администратору для непосредственного исполнения работ по внесению изменений в конфигурацию АРМ или серверов ИС.
   9. В заявке могут быть указаны следующие изменения в составе аппаратных и программных средств АРМ и серверов подразделения:

* установка в подразделении новой ПЭВМ (развертывание новой АРМ или сервера). По данному факту исполнителем заполняется акт установки оборудования (приложение 4);
* замена ПЭВМ (АРМ или сервера подразделения);
* изъятие ПЭВМ (АРМ или сервера подразделения);
* добавление устройства (узла, блока) в состав конкретного АРМ или сервера подразделения;
* замена устройства (узла, блока) в составе конкретного АРМ или сервера подразделения;
* изъятие устройства (узла, блока) из состава конкретного АРМ или сервера;
* обновление (восстановление) системного ПО;
* установка (развертывание) на конкретное АРМ или сервера программных средств, необходимых для решения определенной задачи (добавление возможности решения данной задачи на данном АРМ или сервере), за исключением офисного ПО.
  1. Пользователь обязан обеспечить отделу внедрения автоматизированных систем финансовых расчетов комитета по финансам, налоговой и кредитной политике города Барнаула доступ к оборудованию, включенному в заявку, или организовать транспортировку неисправного оборудования для проведения восстановительных работ.
  2. В случае выявления дефектов СВТ, которые не могут быть устранены собственными силами, СВТ должно быть передано для ремонта в сторонние сертифицированные организации.
  3. Пользователь обязан обеспечить строгое соблюдение правил технической эксплуатации и нормы загрузки оборудования, рекомендованные фирмой-изготовителем, периодическую очистку от пыли и грязи внешних поверхностей оборудования, а также использование оборудования исключительно для решения заявленных производственных задач.
  4. Пользователь не должен допускать случаев привлечения к ТО СВТ третьих лиц либо самостоятельного выполнения таких работ, как установка и настройка системного программного обеспечения, замена комплектующих и материалов, входящих в состав системного оборудования, любые виды работ по системному, сетевому администрированию, а также администрированию систем телекоммуникаций.

1. Перечень работ, входящих в плановое ТО
   1. Компьютеры (сервера, рабочие станции, персональные компьютеры)

5.1.1. Программное обеспечение

5.1.1.1. Проверка установки критически важных обновлений системного программного обеспечения.

5.1.1.2. Проверка работоспособности обновленного системного программного обеспечения.

5.1.1.3. Проверка наличия обновления антивирусного программного обеспечения, наличия вирусов или вредного программного обеспечения и удаления их.

5.1.1.4. Создание архива обновленного системного программного обеспечения.

5.1.1.5. Создание архива данных Пользователя по его просьбе.

5.1.1.6. При невозможности проведения любого из пунктов 5.1.1.1 - 5.1.1.5, допускается полная переустановка системного программного обеспечения из первоначальных дистрибутивов или предыдущих архивов с дальнейшим прохождением этих пунктов.

5.1.2. Аппаратное обеспечение

5.1.2.1. Очистка от пыли внутренних объемов системных устройств. Внешняя чистка системных устройств.

5.1.2.2. Проверка теплового режима системных устройств, в том числе его комплектующих. Комплексная проверка полностью собранного устройства на работоспособность при максимально допустимой внутренней паспортной температуре без основных носителей информации. При необходимости замена термоинтерфейсов.

5.1.2.3. Проверка системы вентиляции на число оборотов и допустимого шума, в том числе системы вентиляции блока питания. При необходимости замена системы вентиляции.

5.1.2.4. Проверка блока питания под нагрузкой. При необходимости произведение ремонта или замена блока питания.

5.1.2.5. Проверка работоспособности устройств со съемными носителями, в том числе на запись, при необходимости чистка специальными носителями или инструментом, ремонт или замена съемного носителя.

5.1.2.6. Проверка используемых портов на работоспособность. При необходимости ремонт или замена используемых портов.

5.1.2.7. Приемо-сдаточная проверка на включение, загрузку, выключение и выборочная проверка по требованию пользователя.

* 1. Принтер:

5.2.1. Приемная проверка работоспособности встроенным тестом печати.

5.2.2. Приемная проверка работоспособности с тестовым сервером печати или компьютером.

5.2.3. Разборка, чистка от пыли, чистка и смазка механизма подачи бумаги, включая термическую часть, чистка печатающей головки / лазерной оптики / чернильных сопел, внутренняя и наружная чистка корпуса; сборка, при необходимости замена изношенных комплектующих и материалов.

5.2.4. Приемо-сдаточная проверка на работоспособность с тестовым сервером печати или компьютером.

* 1. Сканер:

5.3.1. Приемная проверка работоспособности с компьютером.

5.3.2. Разборка, чистка от пыли, чистка и смазка механизма считывания, чистка оптики, внутренняя и наружная чистка корпуса; сборка, при необходимости замена изношенных комплектующих и материалов.

5.3.3. Приемо-сдаточная проверка на работоспособность с компьютером.

* 1. Источник бесперебойного питания:

5.4.1. Приемная проверка работоспособности с компьютером.

5.4.2. Проверка работоспособности источника с батареями под нагрузкой в течение заданного времени.

5.4.3. Проверка процесса зарядки аккумуляторов после разрядки по предыдущему пункту.

5.4.4. Разборка, чистка от пыли, внутренняя и наружная чистка корпуса; сборка, при необходимости замена изношенных комплектующих и материалов.

* 1. Копировально-множительная техника:

5.5.1. Приемная проверка работоспособности путем копирования образца.

5.5.2. Разборка, чистка от пыли, чистка и смазка механизма подачи бумаги, включая термическую часть, чистка лазерной оптики, / чернильных сопел, считывающей оптики, внутренняя и наружная чистка корпуса; сборка, при необходимости замена изношенных комплектующих и материалов.

5.5.3. Приемо-сдаточная проверка на работоспособность путем копирования образца.

* 1. Другие устройства

5.6.1. Приемная проверка работоспособности.

5.6.2. Разборка, чистка от пыли, внутренняя и наружная чистка корпуса; сборка, при необходимости замена изношенных комплектующих и материалов.

5.6.3. Приемо-сдаточная проверка на работоспособность.

1. Состав работ, входящих во внеочередное ТО СВТ
   1. Первичная установка приобретенных средств СВТ, включение их в работу на рабочих местах пользователя.
   2. Передача неисправной техники, находящейся на гарантии, в гарантийный ремонт, получение ее с гарантийного ремонта, и установка на рабочих местах пользователя.
   3. Техническое обслуживание СВТ, не находящихся на гарантийном обслуживании, по заявке пользователя с целью восстановления работоспособности СВТ, устранения последствий его сбоев или отказов.
2. Порядок внесения изменений в конфигурации технических и программных средств ИС
   1. Права и обязанности сотрудников комитета по финансам, налоговой и кредитной политике города Барнаула.

7.1.1.Все изменения должны производиться только на основании заявок начальников отделов, либо системного администратора, либо АИБа. Перечень изменений, на которые требуется оформление заявки, приведен в пункте 4.9 настоящего порядка.

7.1.2.Право внесения изменений в конфигурацию аппаратно-программных средств рабочих станций и серверов ИС, предоставляется:

* в отношении системных и прикладных программных средств –системным администратором;
* в отношении аппаратных средств – системным администратором;
* в отношении программно-аппаратных средств защиты – АИБа;
* в отношении программно-аппаратных средств телекоммуникации – системным администратором;

7.1.3 Установка системного и прикладного программного обеспечения производится в соответствии с Перечнем разрешенного к использованию программного обеспечения (Приложение 5).

7.1.4. Изменение конфигурации аппаратно-программных средств рабочих станций и серверов кем-либо, кроме перечисленных сотрудников, запрещено.

* 1. Ответственные за выполнение разных видов работ

7.2.1. Допускается внесение изменений в состав аппаратных средств и программного обеспечения только при наличии оформленной и согласованной заявки на осуществление данных изменений.

7.2.2. Установка, изменение (обновление) и удаление системных и прикладных программных средств производится системным администратором. Установка, снятие, и внесение необходимых изменений в настройки средств защиты от НСД и средств контроля целостности файлов (при их использовании) на АРМ осуществляется администратором информационной безопасности. В случае необходимости работы производятся в присутствии пользователя данного АРМ.

7.2.3. Подготовка модификаций программного обеспечения защищенных серверов и АРМ, тестирование, стендовые испытания и передача исходных текстов, документации и дистрибутивных носителей программ в архив эталонных дистрибутивов правления и другие необходимые действия производятся системным администртором, согласно утвержденным инструкциям.

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

7.2.5. 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 реализации сетевого архива эталонных дистрибутивов программ – из него). При необходимости (в случае установки части компонент на дисках сетевых серверов) к работам привлекается АИБ.

Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность.

7.2.6. После установки (обновления) ПО АИБ должен произвести настройку СЗИ от НСД, проверить работоспособность ПО и правильность настройки средств защиты.

После завершения работ по внесению изменений в состав аппаратных средств защищаемой АРМ ее системный блок должен быть опечатан (опломбирован, защищен специальной наклейкой) АИБом.

7.2.7. Исполнители работ должны сделать соответствующую запись в формуляре АРМ, отметку о выполнении (на обратной стороне заявки).

7.2.8. Изъятие АРМ из состава рабочих станций подразделения при ее передаче на склад, в ремонт или в другое подразделение осуществляется только после того, как АИБ снимет с данной ПЭВМ средства защиты и предпримет необходимые меры для удаления защищаемой информации, которая хранилась на дисках компьютера. Факт уничтожения данных, находившихся на диске компьютера, оформляется актом за подписью администратора информационной безопасности. В случае поломки жесткого диска при передаче его в организацию для осуществления ремонта, в договоре должна быть предусмотрена ответственность сторонней организации о неразглашении информации, содержащейся на передаваемом диске.

7.2.9. Оригиналы заявок (документов), на основании которых производились изменения в составе технических или программных средств АРМ с отметками о внесении изменений в состав аппаратно-программных средств, должны храниться у АИБа. Они могут использоваться в следующих случаях:

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

7.2.10. Плановое и внеочередное ТО должно отражаться в журнале проверки исправности и технического обслуживания.

1. Экстренная модификация (обстоятельства форс-мажор)
   1. В исключительных случаях (сбой ПО, не позволяющий продолжить работу), требующих безотлагательного изменения ПО, допускается корректировка программ непосредственно на рабочей станции. В данной ситуации системный администратор ставит в известность АИБа о необходимости такого изменения.
   2. Факт внесения изменений в ПО АРМ оформляется актом за подписями пользователя данного АРМ, системного администратора, АИБа. В акте указывается причина модификации, перечисляются файлы, подвергшиеся изменению, и указывается лицо(а), осуществившее изменения. При необходимости проводится изменение ПО загрузочного раздела сервера. Если это необходимо, администратор информационной безопасности вносит необходимые корректировки в настройки системы контроля целостности ПО АРМ и сервера (при их использовании). Факт модификации ПО и корректировок настроек системы защиты фиксируется на АРМ (сервере).
   3. В течение следующего дня после составления акта, АИБ при участии сотрудников технического подразделения выясняют причины и состав проведенных экстренных изменений и принимают решение о необходимости подготовки исправительной модификации ПО или восстановления ПО АРМ (сервера).
   4. Необходимость участия в данном административном расследовании сотрудника подразделения определяется руководством. Результат расследования оформляется в виде согласованного решения и хранится у АИБа.
2. Порядок технического обслуживания и ремонта технических средств АРМ (серверов) ИСПДн
   1. Техническое обслуживание и ремонтные работы на технических средствах ПЭВМ АРМ должны осуществляться только системным администратором, назначенным ответственными за их обслуживание (сопровождение). Их вызов осуществляется сотрудниками подразделения, эксплуатирующих АРМ, при возникновении нештатных ситуаций.
   2. К нештатным ситуациям относятся:

* выход из строя или неустойчивое функционирование узлов ПЭВМ или периферийных устройств (например, дисковода, принтера) АРМ;
* выход из строя системы электроснабжения АРМ.
  1. Техническое обслуживание и регламентные работы могут проводиться в плановом порядке.
  2. Системный администратор имеет право доступа к АРМ для разбора нештатных ситуаций без участия АИБа при обнаружении сбоев в их работе только для тестирования ПЭВМ с использованием установленных на АРМ (в сети) тестовых средств.
  3. Ответственность за соблюдение требований по обеспечению безопасности информации при проведении технического обслуживания и ремонтных работ на ПЭВМ возлагается на администратора информационной безопасности.
  4. При необходимости осуществления изменений аппаратно-программной конфигурации АРМ соответствующие работы выполняются с соблюдением требований данного Порядка.

1. Порядок проверки работоспособности системы защиты после установки (обновления) программных средств внесения изменений в списки пользователей
   1. После установки (обновления) программных средств АРМ или внесения изменений в списки пользователей системы АИБ обязан проверить работоспособность АРМ и правильность настройки средств защиты, установленных на компьютере в соответствии с инструкциями на конкретные СЗИ.
   2. После осуществления данных действий необходимо проверить корректность функционирования системы защиты.