Государственное казенное учреждение здравоохранения
Детский санаторий «ТОПОЛЁК»
Министерства Здравоохранения Краснодарского края

УТВЕРЖДАЮ
Главный врач
ГКУЗ «Детский санаторий «Тополек»
_____ / М. А. Мугу /
«11» 12 2021 г.

ИНСТРУКЦИЯ
ПО УСТАНОВКЕ, МОДИФИКАЦИИ И ТЕХНИЧЕСКОМУ ОБСЛУЖИВАНИЮ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И АППАРАТНЫХ СРЕДСТВ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Настоящей инструкцией регламентируется взаимодействие подразделений ГКУЗ «Детский санаторий «Тополек» по обеспечению безопасности информации при проведении модификаций программного обеспечения, технического обслуживания средств вычислительной техники и при возникновении нештатных ситуаций в работе информационных систем персональных данных (далее – ИСПДн) ГКУЗ «Детский санаторий «Тополек».

Все изменения конфигурации технических и программных средств защищенных рабочих станций (РС) и серверов ИСПДн ГКУЗ «Детский санаторий «Тополек» должны производиться только на основании заявок руководителей структурных подразделений ГКУЗ «Детский санаторий «Тополек», согласованных с ответственным за обеспечение безопасности информации.

Право внесения изменений в конфигурацию аппаратно-программных средств защищенных рабочих станций и серверов ИСПДн ГКУЗ «Детский санаторий «Тополек» предоставляется Администратору безопасности.

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

Право внесения изменений в конфигурацию аппаратно-программных средств РС ИСПДн ГКУЗ «Детский санаторий «Тополек», не требующих защиты, предоставляется как сотрудникам комитета информатизации и связи (на основании служебных записок), так и сотрудникам подразделений, в которых они установлены, на основании распоряжений руководителей данных подразделений.

Процедура внесения изменений в конфигурацию аппаратных и программных средств защищенных серверов и РС системы согласуется с лицом, ответственным за информационную безопасность.

Заявка руководителя подразделения ГКУЗ «Детский санаторий «Тополек», в котором требуется произвести изменения конфигурации РС, оформляется на имя руководителя подразделения, отвечающегоза техническое обслуживание систем. Производственная необходимость проведения указанных в заявке изменений подтверждается подписью Ответственного сотрудника.

Заявка руководителя подразделения, отвечающего за техническоеобслуживание систем, которое отвечает за плановое проведение изменений (обновлений версий) ПО, оформляется на имя руководителя структурного подразделения (подразделений), использующего (использующих) подсистему ИСПДн, требующую модификации. Производственная необходимость проведения указанных в заявке изменений подтверждается подписью Главного врача ГКУЗ «Детский санаторий «Тополек».

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). Наименования задач указываются в соответствии с формулярами задач или перечнем задач архива эталонных дистрибутивов, которые можно решать с использованием ИСПДн.

Заключение о технической возможности осуществления затребованных изменений выдается специалистами подразделения, отвечающего за техническое обслуживание систем, (на основании формуляров задач и формуляров соответствующих РС или серверов).

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

После чего заявка передается в подразделение, отвечающее за техническое обслуживание систем, для непосредственного исполнения работ по внесению изменений в конфигурацию РС или серверов ИСПДн ГКУЗ «Детский санаторий «Тополек».

Ответственный за информационную безопасность в подразделении (при его отсутствии – 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. 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 осуществляется уполномоченными сотрудником ответственным за обеспечение безопасности информации (администратором безопасности). Работы производятся в присутствии ответственного за информационную безопасность 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 ГКУЗ «Детский санаторий «Тополек» и другие необходимые действия производится подразделением, отвечающим за техническое обслуживание систем, согласно утвержденным инструкциям.

Установка или обновление подсистем ИСПДн ГКУЗ «Детский санаторий «Тополек» должны проводиться в строгом соответствии с технологией проведения модификаций программных комплексов данных подсистем.

Модификация ПО на сервере осуществляется уполномоченными сотрудниками подразделения, отвечающего за техническое обслуживание систем, обязательно в присутствии уполномоченного сотрудника ответственного за обеспечение безопасности информации. После установки модифицированных модулей на сервер сотрудник ответственный за обеспечение безопасности информации в присутствии сотрудников подразделения, отвечающего за техническое обслуживание систем, устанавливает защиту целостности модулей на сервере (производит пересчет контрольных сумм эталонов модулей на файл-сервере с помощью средств защиты). После проведения модификации ПО на рабочих станциях сотрудник подразделения, отвечающего за техническое обслуживание систем 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, полученных из архива эталонных дистрибутивов (при реализации сетевого архива эталонных дистрибутивов программ – из него). 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 администратор безопасности (возможно также администраторы серверов и баз данных) должен произвести настройку средств управления доступом к компонентам данной задачи (программного средства) в соответствии с ее (его) формуляром и совместно с сотрудником подразделения, отвечающего за техническое обслуживание систем, и ответственным пользователем РС должен проверить работоспособность ПО и правильность настройки средств защиты.

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

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 специалист ответственный за обеспечение 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.

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 в подразделении (у ответственного за информационную безопасность или руководителя подразделения). Копии заявок и актов могут храниться у ответственного за обеспечение безопасности информации и в подразделении, отвечающем за техническое обслуживание систем. 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

В исключительных случаях (сбой ПО, не позволяющий продолжить работу), требующих безотлагательного изменения ПО, допускается корректировка программ непосредственно на рабочей станции. В данной ситуации сотрудник подразделения, отвечающего за техническое обслуживание систем, ставит в известность Главного врача ГКУЗ «Детский санаторий «Тополек» и ответственного за обеспечение безопасности информации о необходимости такого изменения. Факт внесения изменений в ПО РС фиксируется актом за подписями ответственного за информационную безопасность в подразделении и пользователя данной РС, сотрудников подразделения, отвечающего за техническое обслуживание систем, и ответственного за обеспечение безопасности информации. 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 ответственный за обеспечение безопасности информации вносит необходимые корректировки в настройки системы контроля целостности ПО РС и сервера.

В течение следующего дня после составления акта руководством подразделения, отвечающего за техническое обслуживание систем, и ответственным за обеспечение безопасности информации 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 подразделении, отвечающем за техническое обслуживание систем, копии передаются ответственному за обеспечение безопасности информации и в подразделение.

ПОРЯДОК ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ И РЕМОНТА ТЕХНИЧЕСКИХ СРЕДСТВ РС

Техническое обслуживание и ремонтные работы на технических средствах ПЭВМ РС должны осуществляться только уполномоченными сотрудниками подразделения, отвечающего за техническое обслуживание систем, 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 ответственным за обеспечение безопасности информации заявок.

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 подразделения, отвечающего за техническоеобслуживание систем, имеют право доступа к РС для разбора нештатных ситуаций без участия ответственного за обеспечение безопасности информации при обнаружении сбоев в их работе только для тестирования ПЭВМ с использованием установленных на РС (в сети) тестовых средств.

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 средствам ГКУЗ «Детский санаторий «Тополек».

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 администратор безопасности обязан проверить работоспособность РС и правильность настройки средств защиты, установленных на компьютере.

При установке нового (обновлении существующего) программного средства администратор безопасности обязан:

- установить права доступа пользователей системы к файлам программного средства таким образом, как это указано в формуляре на программное средство (задачу);
- средствами системы СЗИ от НСД 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 СЗИ от НСД 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.