

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

УТВЕРЖДЕН
ВАМБ.00108-06-ЛУ

**СИСТЕМА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
АВТОМАТИЗИРОВАННЫХ СИСТЕМ БАНКА РОССИИ
«ЯНТАРЬ» ВЕРСИЯ 6**

Руководство администратора информационной безопасности

ВАМБ.00108-06 93 01

Аннотация

Данный документ содержит основные правила, связанные с обеспечением информационной безопасности при эксплуатации программного комплекса ВАМБ.00108-06 «Система криптографической защиты информации автоматизированных систем Банка России «Янтарь» версия 6».

Данный документ предназначен для администраторов информационной безопасности и системных администраторов и может служить руководством для разработки в Банке России инструкций администраторам информационной безопасности и пользователям, эксплуатирующим программный комплекс ВАМБ.00108-06 «Система криптографической защиты информации автоматизированных систем Банка России «Янтарь» версия 6». Перед чтением настоящего руководства необходимо ознакомиться с эксплуатационными документами программного комплекса ВАМБ.00108-06 «Система криптографической защиты информации автоматизированных систем Банка России «Янтарь» версия 6», приведёнными в документе ВАМБ.00108-06 20 01 «СКЗИ «Янтарь» версия 6. Ведомость эксплуатационных документов».

Содержание

1 ВВЕДЕНИЕ	4
2 ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ И АДМИНИСТРАТИВНЫЕ МЕРОПРИЯТИЯ	5
2.1 Общие требования	5
2.2 Требования по установке СКЗИ «Янтарь»	6
2.3 Требования по размещению	7
2.4 Защита сетевого взаимодействия	7
2.4.1 Сетевые взаимодействия АРМ УКС и АРМ ФО	8
2.4.2 Сетевые взаимодействия библиотеки ППИ	9
2.4.3 Иные сетевые взаимодействия криптографического сервера	9
2.5 Парольная защита	10
2.6 Требования к антивирусной защите	10
3 НАСТРОЙКА ОС WINDOWS С ЦЕЛЬЮ ЗАЩИТЫ ОТ НСД	11
3.1 Настройка ОС Windows для защиты КС	11
3.2 Настройка ОС Windows для защиты АРМ УКС	13
4 КОНТРОЛЬ ЦЕЛОСТНОСТИ ПО	15
4.1 Перечень файлов ПО КС, подлежащих контролю целостности	15
4.2 Перечень файлов ПО АРМ УКС и АРМ ФО, подлежащих контролю целостности	15
4.3 Перечень файлов библиотеки прикладного программного интерфейса криптографического сервера, подлежащих контролю целостности	16
4.4 Перечень файлов программы тестирования аппаратно-программных средств КС, подлежащих контролю целостности	16
5 КОНТРОЛЬ ПРАВИЛЬНОСТИ РАБОТЫ ЭВМ	17
ПЕРЕЧЕНЬ СОКРАЩЕНИЙ	18

1 ВВЕДЕНИЕ

В организации, эксплуатирующей программный комплекс (ПК) ВАМБ.00108-06 «Система криптографической защиты информации автоматизированных систем Банка России «Янтарь» версия 6» (далее — СКЗИ «Янтарь»), должен быть назначен ответственный за организацию работ по безопасному использованию СКЗИ «Янтарь» (далее — Администратор информационной безопасности).

Примечание — При необходимости функции Администратора информационной безопасности могут быть возложены на нескольких сотрудников или на подразделение.

На Администратора информационной безопасности возлагается:

- создание инструкций, направленных на обеспечение безопасности функционирования СКЗИ «Янтарь», обеспечение пользователей данными инструкциями и контроль за их соблюдением;
- контроль соблюдения требований, описанных в настоящем руководстве и в документе ВАМБ.00107-06 93 01 «СКАД «Сигнатура» версия 6. Средство КЗИ СКАД «Сигнатура» версия 6. Руководство администратора информационной безопасности»;
- контроль выполнения всех вводимых на технологическом участке организационно-технических мер защиты рабочих мест с установленной СКЗИ «Янтарь» от несанкционированного доступа (НСД);
- администрирование программно-аппаратных и программных средств защиты информации от НСД (СЗИ от НСД) на рабочих местах с установленной СКЗИ «Янтарь»;
- контроль выполнения работ по проверке целостности СКЗИ «Янтарь»;
- управление доступом пользователей к программному обеспечению (ПО) и данным, включая установку и периодическую смену паролей;
- определение конкретных настроек ОС и её конфигурирование в целях защиты СКЗИ «Янтарь» от НСД в соответствии с положениями настоящего документа и документа ВАМБ.00107-06 93 01 «СКАД «Сигнатура» версия 6. Средство КЗИ СКАД «Сигнатура» версия 6. Руководство администратора информационной безопасности»;
- анализ содержания журналов СКЗИ «Янтарь» с периодом не более 30 дней.

2 ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ И АДМИНИСТРАТИВНЫЕ МЕРОПРИЯТИЯ

Защита ПО и аппаратного обеспечения от НСД при установке и использовании СКЗИ «Янтарь» является составной частью общей задачи обеспечения безопасности информации в автоматизированных системах и ПК Банка России. Для обеспечения защиты информации от НСД необходимо выполнение целого ряда мер, включающих организационно-технические и административные мероприятия, связанные с обеспечением правильности функционирования технических средств обработки и передачи информации, а также установление соответствующих правил для персонала, администраторов информационной безопасности и пользователей, эксплуатирующих СКЗИ «Янтарь». Защита СКЗИ «Янтарь» от НСД в автоматизированных системах и ПК Банка России должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования СКЗИ «Янтарь», в том числе при проведении ремонтных работ.

2.1 Общие требования

Для защиты ЭВМ с установленной СКЗИ «Янтарь» применяется комплекс организационно-технических мер по оборудованию помещений и обеспечению режима доступа в них, размещению и порядку эксплуатации технических средств.

При эксплуатации СКЗИ «Янтарь» следует принять следующие общие организационные меры:

- должны соблюдаться требования по обеспечению информационной безопасности, изложенные в документе ВАМБ.00107-06 93 01 «СКАД «Сигнатура» версия 6. Средство КЗИ СКАД «Сигнатура» версия 6. Руководство администратора информационной безопасности». В случае функционирования СКЗИ «Янтарь» в виртуальной среде также должны быть выполнены требования, изложенные в документе ВАМБ.00107-06 93 03 «СКАД «Сигнатура» версия 6. Средство КЗИ СКАД «Сигнатура» версия 6. Функционирование в виртуальной среде. Руководство администратора информационной безопасности»;

- право доступа к техническим средствам (далее — ЭВМ) с установленной СКЗИ «Янтарь» предоставляется только лицам, изучившим соответствующие эксплуатационные документы СКЗИ «Янтарь», а также другие документы, созданные на их основе;

- запрещается использование СКЗИ «Янтарь» для защиты сведений, составляющих государственную тайну;

- должны соблюдаться требования по контролю целостности ПО, изложенные в разделе 4 настоящего документа;

- установка ПО на ЭВМ с установленной СКЗИ «Янтарь» должна выполняться с лицензионных копий ПО, полученных официально у поставщика;

- запрещается удаленное подключение к ЭВМ с установленными ПК «Автоматизированное рабочее место управления криптосервером» (АРМ УКС) и ПК

«Автоматизированное рабочее место формирования отчётов» (АРМ ФО) из состава СКЗИ «Янтарь»;

- удаленное подключение к ЭВМ с установленным ПК «Криптографический сервер» (далее — Криптосервер или КС) может выполняться только с ЭВМ, на которой установлен АРМ УКС. Для удаленного подключения к КС необходимо использовать средства удаленного доступа, входящие в состав используемой ОС, при этом защита канала должна обеспечиваться с использованием ключей ЭП и сертификатов АРМ УКС и сессии администрирования с помощью сертифицированных средств криптографической защиты соответствующего класса (не ниже КС1 — для исполнения 1, не ниже КС2 — для исполнения 2), поддерживающих работу с данными ключами ЭП и обеспечивающих шифрование и двухстороннюю аутентификацию с использованием протоколов TLS или IPSec. В этом случае сертификаты АРМ УКС (оператора КС или Администратора АРМ УКС) и сессии администрирования дополнительно должны удовлетворять требованиям к сертификатам, которые предъявляет средство криптографической защиты, используемое для защиты канала связи;

- файловые системы ЭВМ с установленным КС, АРМ УКС и АРМ ФО должны содержать только программные средства, необходимые для эксплуатации соответствующих рабочих мест. Запрещается устанавливать, создавать и выполнять на этих рабочих местах посторонние программы;

- запрещается вносить какие-либо изменения в ПО СКЗИ «Янтарь».

Для обеспечения контроля за доступом к ЭВМ с установленной СКЗИ «Янтарь» дополнительно к мерам, указанным в документе ВАМБ.00107-06 93 01 «СКАД «Сигнатура» версия 6. Средство КЗИ СКАД «Сигнатура» версия 6. Руководство администратора информационной безопасности», необходимо организовать затираание (по окончании сеанса работы СКЗИ «Янтарь») файлов подкачки, формируемых или модифицируемых в процессе работы СКЗИ «Янтарь».

Пользователи должны своевременно ставить Администратора информационной безопасности в известность обо всех инцидентах и подозрительных случаях, произошедших при работе на ЭВМ с установленной СКЗИ «Янтарь».

2.2 Требования по установке СКЗИ «Янтарь»

К установке СКЗИ «Янтарь» допускаются лица, изучившие соответствующую эксплуатационную документацию.

Установка СКЗИ «Янтарь» на ЭВМ должна выполняться с передаточного носителя, поставляемого в виде компакт-диска или в электронном виде. Поставляемые в электронном виде передаточные носители в обязательном порядке должны быть защищены электронной подписью (ЭП). В случае распространения передаточных носителей СКЗИ «Янтарь» в электронном виде в эксплуатирующей организации должны быть назначены сотрудники, ответственные за создание защищённых ЭП передаточных носителей СКЗИ «Янтарь», а также их последующее распространение.

Перед установкой СКЗИ «Янтарь» с передаточного носителя, полученного в виде компакт-диска, должна быть выполнена проверка целостности файлов на

передаточном носителе с использованием программы контроля целостности.

Перед установкой СКЗИ «Янтарь» с передаточного носителя, полученного в электронном виде, должна быть проверена ЭП данного передаточного носителя с использованием ПК ВАМБ.00106-06 «Сигнатура-клиент» версия 6» или иного сертифицированного средства ЭП.

Администратор информационной безопасности должен заблаговременно обеспечить загрузку на ЭВМ, на которой выполняется проверка ЭП полученного в электронном виде передаточного носителя, актуальных сертификатов и списков аннулированных сертификатов (САС), необходимых для проверки ЭП. В случае успешной проверки ЭП Администратор информационной безопасности дополнительно должен убедиться, что сертификат ключа проверки ЭП, использовавшийся для проверки ЭП передаточного носителя, принадлежит сотруднику эксплуатирующей организации, ответственному за создание передаточных носителей в электронном виде.

2.3 Требования по размещению

При эксплуатации, размещении и хранении технических средств с установленной СКЗИ «Янтарь» должен быть обеспечен режим эксплуатации, размещения и хранения технических средств, исключающий несанкционированный доступ к этим техническим средствам. Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать сохранность конфиденциальных документов и сведений, включая ключевую информацию.

При размещении технических средств с установленной СКЗИ «Янтарь» (исполнение 1):

- должны быть приняты меры по исключению доступа в помещения, в которых размещены технические средства, лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в этих помещениях;

- лица, не находящиеся в списке доступа в помещения, в которых размещены технические средства, должны соответствующим образом сопровождаться и контролироваться.

При размещении технических средств с установленной СКЗИ «Янтарь» (исполнение 2):

- должны быть приняты меры по исключению доступа в помещения, в которых размещены технические средства, лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе на этих технических средствах;

- лица, не допущенные к работе на технических средствах, должны соответствующим образом сопровождаться и контролироваться.

2.4 Защита сетевого взаимодействия

Должно быть исключено подключение ЭВМ с установленными КС, АРМ УКС и АРМ ФО к общедоступным сетям связи.

ЭВМ с установленными компонентами СКЗИ «Янтарь» должны размещаться в одной или нескольких контролируемых зонах.

Примечание — Контролируемая зона – это территория или пространство, на которых исключено неконтролируемое пребывание лиц или транспортных

средств без постоянного или разового допуска.

Для СКЗИ «Янтарь» конкретные границы контролируемой зоны определяются исходя из модели угроз эксплуатирующей организации. Для СКЗИ «Янтарь» (исполнение 2) максимально возможной контролируемой зоной является помещение, предназначенное для размещения технических средств с установленной СКЗИ «Янтарь» (исполнение 2).

2.4.1 Сетевые взаимодействия АРМ УКС и АРМ ФО

АРМ УКС из состава СКЗИ «Янтарь» (исполнение 1) должен подключаться к КС одним из следующих способов:

1) при нахождении АРМ УКС и КС в одной контролируемой зоне — путем размещения АРМ УКС и КС в изолированном сегменте локальной вычислительной сети (ЛВС). При этом активное сетевое оборудование, организующее указанный сегмент, должно располагаться на контролируемой территории;

2) в случае размещения АРМ УКС и КС в разных контролируемых зонах канал связи между этими контролируемыми зонами должен быть защищён с использованием средств криптографической защиты сетевого трафика, сертифицированных по классу защиты не ниже, чем класс применяемой СКЗИ «Янтарь». При этом должны соблюдаться следующие требования:

- АРМ УКС и используемое средство криптографической защиты сетевого трафика должны размещаться в изолированном сегменте ЛВС. При этом активное сетевое оборудование, организующее указанный сегмент, должно располагаться на контролируемой территории;

- КС и используемое средство криптографической защиты сетевого трафика должны размещаться в изолированном сегменте ЛВС, при этом активное сетевое оборудование, организующее указанный сегмент, должно располагаться на контролируемой территории.

Подключение АРМ УКС из состава СКЗИ «Янтарь» (исполнение 2) к КС всегда должно защищаться с использованием сертифицированных средств криптографической защиты информации класса не ниже КС2, обеспечивающих шифрование и двустороннюю аутентификацию с использованием протоколов TLS или IPSec. При этом должны соблюдаться следующие требования:

- указанные средства криптографической защиты информации должны функционировать непосредственно на ЭВМ с установленным ПО КС и на ЭВМ с установленным ПО АРМ УКС.

- при размещении АРМ УКС и КС в одной контролируемой зоне подключение должно выполняться посредством изолированного сегмента ЛВС;

- при размещении АРМ УКС и КС в разных контролируемых зонах подключение должно быть защищено с использованием межсетевых экранов (МЭ), удовлетворяющих требованиям документа ВАМБ.00107-06 93 01 «СКАД «Сигнатура» версия 6. Средство КЗИ СКАД «Сигнатура» версия 6. Руководство администратора информационной безопасности». Настройками МЭ должно быть разрешено подключение к КС только с АРМ УКС. При этом соответствующие сегменты сетей от АРМ УКС и КС до соответствующих межсетевых экранов должны быть изолированными. Межсетевые экраны и активное сетевое оборудование,

организующее каждый из указанных сегментов, должны располагаться в пределах соответствующих контролируемых зон.

Иные подключения ЭВМ с установленными АРМ УКС и АРМ ФО, в том числе в целях управления балансировщиком, допускаются только к корпоративной сети по отдельному сетевому интерфейсу. В случае если используемый канал связи выходит за пределы контролируемой зоны, для исключения возможности несанкционированного сетевого доступа к АРМ УКС и АРМ ФО должен использоваться межсетевой экран, удовлетворяющий требованиям документа ВАМБ.00107-06 93 01 «СКАД «Сигнатура» версия 6. Средство КЗИ СКАД «Сигнатура» версия 6. Руководство администратора информационной безопасности».

2.4.2 Сетевые взаимодействия библиотеки ППИ

К подключению центра обработки информации (ЦОИ), использующего библиотеку прикладного программного интерфейса криптографического сервера из состава СКЗИ «Янтарь» (далее — библиотека ППИ), к КС предъявляются те же требования, что и для подключения АРМ УКС к КС. При этом все используемые для связи КС с АРМ УКС и КС с ЦОИ изолированные сегменты ЛВС должны быть попарно различны.

Допускается подключение ЦОИ к общедоступным сетям связи с использованием сегмента ЛВС, отличного от используемого для связи ЦОИ с КС. Также должны быть предприняты дополнительные меры, исключающие возможность несанкционированного доступа к системным ресурсам используемых ОС, к ПО, в окружении которого функционирует СКЗИ «Янтарь», и к компонентам СКЗИ «Янтарь» со стороны указанных сетей.

2.4.3 Иные сетевые взаимодействия криптографического сервера

Если для функционирования КС требуются подключения к маршрутизируемым сетям (например, для взаимодействия с сетевым справочником сертификатов, серверами штампов времени и проверки статуса сертификата, точками доступа к Центру (AIA) и распространения САС (CDP)), такие подключения должны выполняться посредством выделенных сетевых интерфейсов, не используемых для связи КС с ЦОИ и КС с АРМ УКС, с выполнением следующих требований для каждого такого сетевого интерфейса:

- подключение допускается только к корпоративной сети и с использованием межсетевого экрана, удовлетворяющего требованиям документа ВАМБ.00107-06 93 01 «СКАД «Сигнатура» версия 6. Средство КЗИ СКАД «Сигнатура» версия 6. Руководство администратора информационной безопасности»;

- сегмент сети между КС и межсетевым экраном должен быть изолирован от сегментов других сетей;

- настройками межсетевого экрана должны быть разрешены исключительно исходящие от КС подключения, и только те, которые необходимы для функционирования КС. Все входящие подключения к КС настройками межсетевого экрана должны быть запрещены.

2.5 Парольная защита

При использовании парольных механизмов ОС на ЭВМ с установленной СКЗИ «Янтарь» необходимо разработать и применить политику назначения и смены паролей (для входа в ОС, BIOS/UEFI и т.д.), руководствуясь соответствующими нормативными документами эксплуатирующей организации и правилами, изложенными в документе ВАМБ.00107-06 93 01 «СКАД «Сигнатура» версия 6. Средство КЗИ СКАД «Сигнатура» версия 6. Руководство администратора информационной безопасности». При этом максимальное число неудачных попыток ввода пароля должно быть не более 10. При превышении числа неудачных попыток ЭВМ должна быть заблокирована на период не менее одной минуты или до перезагрузки (устанавливается при настройке параметров безопасности ОС).

2.6 Требования к антивирусной защите

При создании информационной системы, защищаемой с использованием шифровальных (криптографических) средств, необходимость применения антивирусных средств в создаваемой информационной системе определяется на основании модели угроз и нарушителя для данной системы. Если такая необходимость определена, должны применяться антивирусные средства, одобренные федеральным органом исполнительной власти, ответственным за обеспечение информационной безопасности в создаваемой информационной системе.

3 НАСТРОЙКА ОС WINDOWS С ЦЕЛЬЮ ЗАЩИТЫ ОТ НСД

3.1 Настройка ОС Windows для защиты КС

Учетные записи пользователей в ОС Windows

На ЭВМ с установленным КС необходимо завести следующие учетные записи пользователей в ОС Windows:

- Системный администратор — член группы «Администраторы» (Administrators). В группу «Администраторы» могут входить только пользователи с эксплуатационной ролью «Системный администратор»;
- Администратор криптосервера (по количеству физических лиц, допущенных к запуску криптосервера) — члены группы «Пользователи» (Users);
- Оператор криптосервера — члены группы «Пользователи» (Users).

Операция заведения учетных записей производится системным администратором.

Настройки прав доступа

Права на управление аудитом и журналом безопасности должны быть предоставлены только группе «Администраторы» (контролируется системным администратором из программы «Редактор локальной групповой политики», меню Политика «Локальный компьютер»→Конфигурация компьютера→Конфигурация Windows→Параметры безопасности→Локальные политики→Назначение прав пользователя→Управление аудитом и журналом безопасности).

Права доступа к каталогу с журналами криптосервера (включая файлы):

- для субъекта «СИСТЕМА» (SYSTEM) — изменение (Change);
- для всех пользователей (Everyone) — чтение (Read);
- для системного администратора — полный доступ (Full control).

Установка данных прав контролируется при помощи программы gpedit.msc из состава ОС Windows. Также, при необходимости, права могут быть установлены вручную. Операция производится системным администратором после установки ПО КС и создания ключевой системы криптосервера.

Задание аудита на критичные события производится системным администратором после задания необходимых прав доступа.

Общесистемный аудит на события:

- вход и выход;
- управление пользователями и группами;
- изменение политики информационной безопасности;
- включение и выключение системы.

Аудит на каталог с ключами криптосервера:

- протоколировать все действия групп «Пользователи» и «Администраторы».

Примечание — Под термином «Каталог с ключами» понимается каталог, где находятся файлы local.pse и local.gdbm (при их наличии).

Аудит на каталог с журналами криптосервера:

- протоколировать следующие действия групп «Пользователи» и «Администраторы»:

- Запись (Write);
- Удаление (Delete);
- Смена разрешений (Change permissions);
- Смена владельца (Take ownership).

Права на запуск и остановку сервисов КС пользователям, допущенным к запуску криптосервера

Для назначения пользователю или группе прав на запуск и остановку сервисов КС необходимо выполнить следующие команды:

а) получить SID пользователя:

– wmic useraccount where name='<Имя пользователя>' get name,sid — для локального пользователя;

– wmic useraccount where (name='<Имя пользователя>' and domain='%userdomain%') get name,domain,sid — для доменного пользователя;

б) получить SID группы:

– wmic group where name='<Имя группы>' get name,sid — для локальной группы;

– wmic group where (name='<Имя группы>' and domain='%userdomain%') get name,domain,sid — для доменной группы;

в) назначить права для запуска сервисов:

– запуск сервиса CryptoServer Logger — СКЗИ «Янтарь»

SC.EXE SDSET cslogsvc D:(A;;RPWPCR;;;<SID пользователя или SID группы>)(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU) S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)

– запуск сервиса CryptoServer Service — СКЗИ «Янтарь»

SC.EXE SDSET cssvc D:(A;;RPWPCR;;;<SID пользователя или SID группы>)(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU) S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)

3.2 Настройка ОС Windows для защиты АРМ УКС

Учетные записи пользователей в ОС Windows

На ЭВМ с установленным АРМ УКС необходимо завести следующие учетные записи пользователей в ОС Windows:

- Системный администратор — член группы «Администраторы» (Administrators). В группу «Администраторы» могут входить только пользователи с эксплуатационной ролью «Системный администратор»;
- Администратор АРМ УКС (по количеству физических лиц — администраторов АРМ УКС) — член группы «Пользователи».

Операция производится системным администратором.

Настройки прав доступа

Права на управление аудитом и журналом безопасности должны быть предоставлены только группе «Администраторы» (контролируется системным администратором из программы «Редактор локальной групповой политики», меню Политика «Локальный компьютер»→Конфигурация компьютера→Конфигурация Windows→Параметры безопасности→Локальные политики→Назначение прав пользователя→Управление аудитом и журналом безопасности).

Права доступа к каталогу с ключами каждого администратора АРМ УКС (включая подкаталоги и файлы):

- для владельца (администратора АРМ УКС) — полный доступ (Full control);
- для системного администратора — специальный доступ к каталогам.

Примечание — Под термином «Каталог с ключами» понимается каталог, где находятся файлы local.pse и local.gdbm (при их наличии).

Для настройки специального доступа системному администратору к каталогам необходимо установить разрешения/запреты, приведенные ниже (Таблица 1) в свойствах каталога с ключами.

Таблица 1 – Настройка специального доступа системному администратору

Разрешения	Разрешить	Запретить
Полный доступ		
Обзор файлов / Выполнение файлов	✓	
Содержание папки / Чтение данных	✓	
Чтение атрибутов	✓	
Чтение дополнительных атрибутов	✓	
Создание файлов / Запись данных		✓
Создание папок / Дозапись данных		✓
Запись атрибутов		✓
Запись дополнительных атрибутов		✓
Удаление подпапок и файлов		✓
Удаление		✓
Чтение разрешений		✓
Смена разрешений		✓
Смена владельца		✓

Рекомендуется проконтролировать установку данных прав при помощи программы gpedit.msc из состава ОС Windows. Также, при необходимости, права могут быть установлены вручную. Операция производится каждым администратором АРМ УКС для своего ключевого каталога при консультационной поддержке системного администратора.

Задание аудита на критичные события производится системным администратором после задания необходимых прав доступа.

Общесистемный аудит на события:

- вход и выход;
- управление пользователями и группами;
- изменение политики информационной безопасности;
- включение и выключение системы.

Аудит на каталог с ключами каждого администратора АРМ УКС:

- протоколировать все действия всех пользователей (Everyone).

4 КОНТРОЛЬ ЦЕЛОСТНОСТИ ПО

При использовании СКЗИ «Янтарь» необходимо организовать в соответствии с требованиями документа ВАМБ.00107-06 93 02 «СКАД «Сигнатура» версия 6. Средство КЗИ СКАД «Сигнатура» версия 6. Программа контроля целостности. Руководство администратора информационной безопасности» контроль целостности следующих объектов:

- системного ПО;
- ПК ВАМБ.00107-06 «Средство КЗИ СКАД «Сигнатура» версия 6» (далее — ПК «Средство КЗИ»);
- ПК ВАМБ.00106-06 «Сигнатура-клиент» версия 6»;
- СКЗИ «Янтарь»;
- прикладного ПО, в которое встраивается СКЗИ «Янтарь»;
- ПО средств виртуализации (при функционировании в виртуальной среде).

В настоящем разделе приведены списки модулей ПО СКЗИ «Янтарь», подлежащих контролю целостности. Для ПК, функционирующих совместно с СКЗИ «Янтарь», перечень файлов, подлежащих контролю целостности, приведён в эксплуатационной документации соответствующих ПК. Списки модулей системного ПО и ПО средств виртуализации, подлежащих контролю целостности, приведены в документе ВАМБ.00107-06 93 01 «СКАД «Сигнатура» версия 6. Средство КЗИ СКАД «Сигнатура» версия 6. Руководство администратора информационной безопасности». Список подлежащих контролю целостности файлов, расположенных в системном каталоге ОС, приведён в документе ВАМБ.00106-06 93 01 «СКАД «Сигнатура» версия 6. «Сигнатура-клиент» версия 6. Руководство администратора информационной безопасности».

4.1 Перечень файлов ПО КС, подлежащих контролю целостности

В каталоге, в который установлено ПО КС (по умолчанию `%ProgramFiles%\MDPREI\spki` или `%ProgramFiles(x86)%\MDPREI\spki`):

- `scssvc.exe`;
- `cslogsvc.exe`;
- `scsmon.exe`;
- `csmgmt.dll`.

4.2 Перечень файлов ПО АРМ УКС и АРМ ФО, подлежащих контролю целостности

В каталоге, в который установлено ПО АРМ УКС и АРМ ФО (по умолчанию `%ProgramFiles%\MDPREI\spki` или `%ProgramFiles(x86)%\MDPREI\spki`):

- `scsadm.exe`;
- `vcertfn.dll`;

- armfo.exe;
- armfo_.xsl;
- armfo1.xsl;
- crypto.xsl.

4.3 Перечень файлов библиотеки прикладного программного интерфейса криптографического сервера, подлежащих контролю целостности

1) В системном каталоге ОС (%WINDIR%\system32 или %WINDIR%\System\Win\System64):

- libpki1.dll.

2) В каталоге, в который установлена библиотека ППИ (по умолчанию %ProgramFiles%\MDPREI\crsrvsdk\bin или %ProgramFiles(x86)%\MDPREI\crsrvsdk\bin):

- pki1utl.exe.

4.4 Перечень файлов программы тестирования аппаратно-программных средств КС, подлежащих контролю целостности

В каталоге, в который установлена библиотека ППИ (по умолчанию %ProgramFiles%\Validata\hdtest или %ProgramFiles(x86)%\Validata\hdtest):

- hdtest.exe;
- hdstop.dll;
- hdts01.dll;
- hdts02.dll;
- hdts03.dll;
- hdts04.dll;
- hdtest.cfg;
- List.Hash(x86).txt или List.Hash(x64).txt;
- validata.url.

5 КОНТРОЛЬ ПРАВИЛЬНОСТИ РАБОТЫ ЭВМ

Для обеспечения контроля правильности работы ЭВМ с установленной СКЗИ «Янтарь» необходимо с периодом не более 168 часов (7 суток) производить перезагрузку работающей ЭВМ с установленной СКЗИ «Янтарь».

При этом перезагрузку работающей ЭВМ необходимо производить с отключением и последующим включением питания ЭВМ с целью выполнения встроенных в постоянное запоминающее устройство ЭВМ тестов проверки работоспособности аппаратных ресурсов. В случае когда после отключения питания ЭВМ дальнейшей работы с данной ЭВМ не требуется, производить перезагрузку не требуется.

Если условия эксплуатации КС требуют непрерывной работы ЭВМ в течение длительного времени (более 7 суток), допустимо осуществлять перезагрузку ЭВМ с установленным ПО КС с периодом не более одного года при обязательном выполнении следующих условий:

- на ЭВМ должна быть установлена серверная ОС;
- должны использоваться ЭВМ с оперативным запоминающим устройством (ОЗУ) со встроенными средствами, обеспечивающими обнаружение и исправление ошибок памяти при сбоях ОЗУ (как минимум, с контролем четности);
- должен быть организован периодический, не реже одного раза в сутки, контроль целостности ПО КС, системного и прикладного ПО с помощью программы контроля целостности из состава ПК «Средство КЗИ» или программы тестирования аппаратно-программных средств криптографического сервера из состава СКЗИ «Янтарь»;
- должно быть организовано периодическое, не реже одного раза в сутки, тестирование корректности работы процессора с использованием программы тестирования аппаратно-программных средств криптосервера из состава СКЗИ «Янтарь».

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АРМ УКС	Автоматизированное рабочее место управления крипто- графическим сервером
АРМ ФО	Автоматизированное рабочее место формирования от- чётов
КС	Криптографический сервер
ЛВС	Локальная вычислительная сеть
НСД	Несанкционированный доступ
ОЗУ	Оперативное запоминающее устройство
ОС	Операционная система (Operating System)
ПК	Программный комплекс
ПО	Программное обеспечение
СКАД	Система криптографической авторизации электронных документов
СКЗИ	Система криптографической защиты информации
Средство КЗИ	Средство криптографической защиты информации
ЦОИ	Центр обработки информации
ЭВМ	Электронно-вычислительная машина
ЭП	Электронная подпись

[illegible][illegible]