

ООО «ВАЛИДАТА»

УТВЕРЖДЕН
ВАМБ.00077-06-ЛУ

«ВАЛИДАТА КЛИЕНТ» ВЕРСИЯ 4

Руководство администратора информационной безопасности

ВАМБ.00077-06 93 01

2020

Аннотация

Данный документ содержит основные правила, связанные с обеспечением информационной безопасности при эксплуатации программного комплекса ВАМБ.00077-06 «“Валидата Клиент” версия 4».

Данный документ предназначен для администраторов информационной безопасности и системных администраторов и может служить руководством для разработки инструкций администраторам информационной безопасности и пользователям, эксплуатирующим программный комплекс ВАМБ.00077-06 «“Валидата Клиент” версия 4». Перед чтением настоящего руководства необходимо ознакомиться с эксплуатационными документами программного комплекса ВАМБ.00077-06 «“Валидата Клиент” версия 4», приведёнными в документе ВАМБ.00077-06 20 01 «“Валидата Клиент” версия 4. Ведомость эксплуатационных документов».

Содержание

1 ВВЕДЕНИЕ	4
2 ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ И АДМИНИСТРАТИВНЫЕ МЕРОПРИЯТИЯ	5
2.1 Общие требования	5
2.2 Требования по установке ПК «Валидата Клиент»	6
3 КОНТРОЛЬ ЦЕЛОСТНОСТИ ПО	7
4 КОНТРОЛЬ ПРАВИЛЬНОСТИ РАБОТЫ ЭВМ	10
ПЕРЕЧЕНЬ СОКРАЩЕНИЙ	11

1 ВВЕДЕНИЕ

В организации, эксплуатирующей программный комплекс (ПК) ВАМБ.00077-06 «Валидата Клиент» версия 4» (далее — ПК «Валидата Клиент»), должен быть назначен ответственный за организацию работ по безопасному использованию ПК «Валидата Клиент» (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 ПК «Валидата Клиент», доведение данных инструкций до пользователей и контроль за их соблюдением;
- контроль соблюдения требований, описанных в настоящем руководстве и в документе ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности»;
- контроль выполнения всех вводимых на технологическом участке организационно-технических мер защиты рабочих мест с установленным ПК «Валидата Клиент» от несанкционированного доступа (НСД);
- администрирование программно-аппаратных и программных средств защиты информации от НСД (СЗИ от НСД) на рабочих местах с установленным ПК «Валидата Клиент»;
- контроль выполнения работ по проверке целостности ПК «Валидата Клиент»;
- управление доступом пользователей к программному обеспечению (ПО) и данным, включая установку и периодическую смену паролей;
- анализ содержания журналов ПК «Валидата Клиент» с периодом не более 30 дней.

2 ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ И АДМИНИСТРАТИВНЫЕ МЕРОПРИЯТИЯ

Защита ПО и аппаратного обеспечения от НСД при установке и использовании ПК «Валидата Клиент» является составной частью общей задачи обеспечения безопасности информации в автоматизированных системах и ПК эксплуатирующей организации. 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 ПК «Валидата Клиент». Защита ПК «Валидата Клиент» от НСД в автоматизированных системах и ПК эксплуатирующей организации должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования ПК «Валидата Клиент», в том числе при проведении ремонтных работ.

2.1 Общие требования

При эксплуатации ПК «Валидата Клиент» следует принять следующие общие организационные меры:

- должны соблюдаться требования по обеспечению информационной безопасности, изложенные в документе ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности». В случае функционирования ПК «Валидата Клиент» в виртуальной среде также должны быть выполнены требования, изложенные в документе ВАМБ.00060-06 93 03 «СКЗИ «Валидата CSP» версия 6. Функционирование в виртуальной среде. Руководство администратора информационной безопасности»;

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

- запрещается использование ПК «Валидата Клиент» для защиты сведений, составляющих государственную тайну;

- должны соблюдаться требования по контролю целостности ПО, изложенные в разделе 3 настоящего документа;

- установка ПО должна выполняться с лицензионных копий ПО, полученных официально у поставщика;

- запрещается вносить какие-либо изменения в ПО ПК «Валидата Клиент».

Для защиты ЭВМ с установленным ПК «Валидата Клиент» применяется комплекс организационно-технических мер по оборудованию помещений и обеспечению режима доступа в них, размещению и порядку эксплуатации технических средств.

Для обеспечения контроля за доступом к ЭВМ с установленным ПК «Валидата Клиент» дополнительно к мерам, указанным в документе ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности», необходимо организовать затирание (по окончании сеанса работы ПК «Валидата Клиент») файлов подкачки, формируемых или модифицируемых в процессе работы ПК «Валидата Клиент».

В случае использования на ЭВМ ПК «АК СКЗИ» или ПК «СК СКЗИ. Сервис» из состава ПК «Валидата Клиент» дополнительно необходимо выполнять следующие требования:

- пользователь ПК «АК СКЗИ» или ПК «АК СКЗИ. Сервис» не должен иметь доступ к папкам, используемых в работе других пользователей ПК «АК СКЗИ» или ПК «АК СКЗИ. Сервис»;
- иные пользователи ОС Windows, не имеющие административных привилегий, не должны иметь доступа к папкам пользователей ПК «АК СКЗИ» или ПК «АК СКЗИ. Сервис».

Пользователи должны своевременно ставить Администратора информационной безопасности в известность обо всех инцидентах и подозрительных случаях, произошедших при работе на ЭВМ с установленным ПК «Валидата Клиент».

2.2 Требования по установке ПК «Валидата Клиент»

К установке ПК «Валидата Клиент» допускаются лица, изучившие соответствующую эксплуатационную документацию.

Установка ПК «Валидата Клиент» на ЭВМ должна выполняться с передаточного носителя, поставляемого в виде оптического диска или в электронном виде. Поставляемые в электронном виде передаточные носители в обязательном порядке должны быть защищены электронной подписью (ЭП).

Перед установкой ПК «Валидата Клиент» с передаточного носителя, полученного в виде оптического диска, должна быть выполнена проверка целостности файлов на передаточном носителе с использованием программы контроля целостности.

Перед установкой ПК «Валидата Клиент» с передаточного носителя, полученного в электронном виде, должна быть проверена ЭП данного передаточного носителя с использованием ПК «Валидата Клиент» 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, необходимых для проверки ЭП.

3 КОНТРОЛЬ ЦЕЛОСТНОСТИ ПО

При использовании ПК «Валидата Клиент» необходимо организовать в соответствии с требованиями документа ВАМБ.00060-06 93 02 «СКЗИ «Валидата CSP» версия 6. Контроль целостности. Руководство администратора информационной безопасности» контроль целостности следующих объектов:

- системного ПО;
- ПК ВАМБ.00060-06 «СКЗИ «Валидата CSP» версия 6»;
- ПК «Валидата Клиент»;
- прикладного ПО, в которое встраивается ПК «Валидата Клиент»;
- ПО средств виртуализации (при функционировании в виртуальной среде).

Ниже приведены списки модулей ПК «Валидата Клиент», подлежащих контролю целостности. Для ПК, функционирующих совместно с ПК «Валидата Клиент», 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.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности».

В системном каталоге ОС:

- zпки.dll;
- zpkissl.dll;
- zcertui.dll;
- zпки1.dll;
- zpkicom.dll;
- vc pia2.dll;
- gdbm10.dll;
- intl10.dll;
- iconv10.dll;
- libxml210.dll;
- msvcr100.dll;
- mfc100.dll;
- vcertmsg.dll;
- mfcм100.dll;
- msvcp100.dll;
- vcomp100.dll;
- atl100.dll;
- zпки.mo (в каталоге
%WINDIR%/LC_MESSAGES/ru_
RU);
- zpkissl.dll.

В каталоге, в который установлен ПК «Справочник сертификатов»:

- zcs.exe;
- zпки1utl.exe;
- stunnel.exe;
- skzi_info.exe.

В дополнение к приведенному перечню в список контроля целостности необходимо внести следующие файлы:

В каталоге, в который установлен ПК «Автоматизированный клиент СКЗИ» (по умолчанию %WINDIR%\Validata\zpkitray):

- CIPT AC - handler.exe;
- CIPT AC - configuration.exe;
- zlibwapi.dll;

В каталоге, в который установлен ПК «Автоматизированный клиент СКЗИ. Монитор» (по умолчанию %WINDIR%\Validata\zpkitraymonitor):

- CIPT AC - monitor.exe;

В каталоге, в который установлен ПК «Автоматизированный клиент СКЗИ. Сервис» (по умолчанию %WINDIR%\Validata\zpkiservice):

- zpkiservice.exe;

- CIPT AC SERVICE - configuration.exe;
- zlibwapi.dll;

В каталоге, в который установлен ПК «Автоматизированный клиент СКЗИ. Сервис монитор» (по умолчанию %WINDIR%\Validata\zpkiservicemonitor):

- CIPT AC - monitor.exe;

В каталоге, в который установлена программа TLSProxy (по умолчанию %WINDIR%\Validata\Validata TLSProxy):

- ztlsproxy.

4 КОНТРОЛЬ ПРАВИЛЬНОСТИ РАБОТЫ ЭВМ

Для обеспечения контроля правильности работы ЭВМ с установленным ПК «Валидата Клиент» необходимо с периодом не более 168 часов (7 суток) производить перезагрузку работающей ЭВМ с установленным ПК «Валидата Клиент».

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 ПК «Валидата Клиент» требуют непрерывной работы ЭВМ в течение длительного времени (более 7 суток), допустимо осуществлять перезагрузку ЭВМ с установленным ПК «Валидата Клиент» 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 ПК «Валидата Клиент», ПК, функционирующих совместно с ПК «Валидата Клиент», системного и прикладного ПО с помощью программы контроля целостности из состава ПК «Валидата Клиент» или программы тестирования аппаратно-программных средств криптографического сервера ВАМБ.00096-06 12 07 (компонент, входящий в состав ПК ВАМБ.00096-06 «Средство криптографической защиты информации «Валидата Криптосервер» версия 4»);
- должно быть организовано периодическое, не реже одного раза в сутки, тестирование корректности работы процессора с использованием программы тестирования аппаратно-программных средств криптосервера ВАМБ.00096-06 12 07.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

НСД	Несанкционированный доступ
ОС	Операционная система (Operating System)
ПК	Программный комплекс
ПО	Программное обеспечение
ЭВМ	Электронно-вычислительная машина
ЭП	Электронная подпись (Digital Signature)

[illegible][illegible]