ГАЗИНФОРМ СЕРВИС

Средство доверенной загрузки «SafeNode System Loader»

Описание применения

Санкт-Петербург, 2018

Аннотация

Настоящий документ содержит сведения о применении средства доверенной загрузки «SafeNode System Loader» (далее по тексту – изделие).

В разделе «Назначение изделия» дан краткий обзор основных функциональных возможностей СДЗ «SafeNode System Loader».

В разделе «Условия применения» указаны условия, необходимые для использования изделия, а также минимальные требования к ЭВМ для установки изделия.

В соответствующих разделах указаны задачи по защите информации, которые решает изделие, и функции, с помощью которых эти задачи решаются, а также описаны виды входных и выходных данных для основных функций изделия.

Содержание

1 Назначение изделия

1.1 Средство доверенной загрузки (СДЗ) «SafeNode System Loader» является разработкой ООО «Газинформсервис» представляет собой программно-техническое средство, встраиваемое в базовую систему ввода-вывода электронно-вычислительной машины (ЭВМ) и обеспечивающее невозможность подключения нарушителя в разрыв между базовой системой ввода-вывода и СДЗ для несанкционированного доступа.

1.2 Изделие обеспечивает доверенную загрузку операционных систем (ОС), установленных на совместимые с архитектурой Intel x86-64 ЭВМ.

1.3 Изделие предназначено для эксплуатации в составе ЭВМ, совместимых с архитектурой Intel x86-64.

1.4 Программные модули изделия выполняют следующие функции СДЗ:

- идентификация пользователей с помощью уникальных учетных записей и соответствующих им паролей;
- идентификация пользователей с помощью уникальных учетных записей и соответствующих им паролей;
- аутентификация пользователей с использованием АНП и уникальных PIN-кодов к ним. Поддерживается работа со следующими АНП[1]:
  - JaCarta PKI, JaCarta ГОСТ (USB-носитель и смарт-карта), JaCarta PKI/ГОСТ, JaCarta-2 ГОСТ (USB-носитель и смарт-карта);
  - Рутокен ЭЦП, Рутокен ЭЦП 2.0 (USB-носитель и смарт-карта), Рутокен Lite, Рутокен 2151, Рутокен ЭЦП PKI (смарт-карта);
  - eToken Pro Java;
  - SafeNet eToken 5100, SafeNet eToken 5105, SafeNet eToken 5200, SafeNet eToken 5205.
- блокировка загрузки пользователями нештатных копий ОС;
- блокировка возможности обхода процесса доверенной загрузки с помощью внешних органов управления;
- обеспечение защищенности паролей пользователей и PIN-кодов при выполнении операций их ввода-вывода;
- контроль целостности: объектов файловой системы, каталогов, объектов реестра ОС семейства Microsoft Windows, аппаратных устройств ЭВМ, загрузочных секторов устройств хранения данных, переменных и драйверов среды UEFI, таблиц

[1] В таблице 1 приведено соответствие между применяемыми идентификаторами и грифами секретности защищаемой с их помощью информации.

ACPI и SMBIOS, завершенности транзакций журналов файловых систем NTFS, EXT3, EXT4;

- блокировка доверенной загрузки ОС при нарушении пользователями установленных политик безопасности (нарушения политик контроля целостности, аутентификации);
- доверенная загрузка ОС, установленных на совместимые с архитектурой Intel x86-64 ЭВМ;
- доверенная загрузка ОС семейств Linux/Unix, поддерживающих стандарт Linux Standard Base (LSB) версии не ниже 3.0, в том числе систем виртуализации VMware ESX, VMware ESXi, установленных на совместимые с архитектурой Intel x86-64 ЭВМ;
- доверенная загрузка ОС на ЭВМ с интерфейсами EFI/UEFI (спецификация UEFI версии не ниже 2.0);
- регистрация событий в журнале событий о действиях пользователей и администратора безопасности (АБ);
- диагностика программных средств изделия.

Таблица 1 – Уровни конфиденциальности информации при использовании идентификаторов

№ п/п	Наименование	Производитель	Сведения о сертификате	Гриф секретности	Примечание
1	eToken	ЗАО «АЛАДДИН Р.Д.»	Сертификат ФСТЭК России № 1883	КИ	
2	JaCarta		Сертификат ФСТЭК России № 3449	КИ	
3	SafeNet eToken	ЗАО «СИС»	Сертификат ФСТЭК России № 2730	КИ	
4	Рутокен (Rutoken)	АО «Актив Софт»	Сертификат ФСТЭК России № 1461	С	
5			Сертификат ФСТЭК России № 2584	КИ	
6			Сертификат ФСТЭК России № 2589	КИ	

1.5 Функции безопасности изделия соответствуют требованиям:

- руководящего документа (РД) «Требования к средствам доверенной загрузки» (ФСТЭК России, 2013);
- методического документа «Профиль защиты средства доверенной загрузки уровня базовой системы ввода-вывода второго класса защиты ИТ.СДЗ.УБ2.ПЗ» (ФСТЭК России, 2013).

1.6 Программное обеспечение (ПО) изделия поддерживает работу с загрузчиками ОС и файловыми системами, указанными в таблице 2.

Таблица 2 – Список поддерживаемых загрузчиков и файловых систем

Семейство ОС	Тип загрузчика ОС	Файл загрузчика ОС	Тип файловой системы
Windows	Windows Boot Manager	Master Boot Record (MBR) …\EFI\BOOT\BOOTX64.EFI …\EFI\Microsoft\Boot\bootmgfw.efi	FAT32, NTFS
Unix	LInux LOader (LILO)	MBR	Ext2, Ext3, Ext4, FAT32, UDF
	Grand Unified Bootloader (GRUB)	…\EFI\BOOT\BOOTX64.EFI	
Linux	LILO	MBR …\EFI\BOOT\BOOTX64.EFI	Ext2, Ext3, Ext4, FAT32, UDF
	GRUB	…\EFI\BOOT\BOOTX64.EFI …\EFI\BOOT\FBX64.EFI …\EFI\BOOT\grubx64.efi …\EFI\CENTOS\GRUBX64.EFI …\EFI\CENTOS\SHIM.EFI …\EFI\CENTOS\SHIMX64.EFI …\EFI\CENTOS\shimx64-centos.efi …\EFI\redhat\grubx64.efi …\EFI\redhat\shim.efi …\EFI\redhat\shimx64.efi …\EFI\redhat\shimx64-redhat.efi …\EFI\ubuntu\grubx64.efi …\EFI\ubuntu\shimx64.efi	
VMware ESX, VMware ESXi	LILO	MBR …\EFI\BOOT\BOOTX64.EFI	Ext2, Ext3, Ext4, FAT32, UDF
	GRUB	MBR …\EFI\BOOT\BOOTX64.EFI	Ext2, Ext3, Ext4, FAT32, UDF

1.7 После установки изделия и его первичной настройке согласно руководству по установке АБ доступны три варианта исполнения консоли управления параметрами СДЗ:

- **псевдографическая консоль СДЗ**, исполняемая в среде **UEFI BIOS** и запускаемая по требованию АБ (**консоль АБ**). Доступна АБ только после успешного прохождения их процедуры аутентификации и идентификации после включения питания ЭВМ и старте ПО изделия;
- **графическая консоль СДЗ Linux (консоль АБ Linux)**, запускаемая по требованию АБ в составе ОС **Linux** (ОС входит в комплект поставки изделия). Не

требует установки дополнительных библиотек и утилит для работы. При запуске не требуется аутентификация и идентификация АБ, так как запуск данной консоли возможен только АБ из псевдографической консоли СДЗ;

- **графическая консоль СДЗ Windows (консоль АБ Windows)**, запускаемая по требованию АБ из среды ОС **Windows**. Не требует установки дополнительных библиотек и утилит для работы. Для запуска консоли и управления параметрами СДЗ требуется обязательная аутентификация и идентификация АБ.

1.8 База данных изделия является единой для всех консолей АБ.

1.9 Различия в настройке консолей АБ приведены в следующей эксплуатационной документации на изделие:

- «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 2. Руководство администратора. ГМТК.468269.060РЭ2»;
- «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 3. Руководство администратора Linux/Windows. ГМТК.468269.060РЭ3».

1.10 Для удобства конфигурирования параметров изделия в каждом варианте исполнения консоли возможны расширенный и сокращенный режим отображения элементов, который устанавливается самостоятельно АБ.

2 Условия применения

2.1 Требования к эксплуатации

2.1.1 Для установки изделия ЭВМ должна иметь следующий минимальный состав технических и программных средств:

- материнская плата ЭВМ с процессором архитектуры **Intel x86-64** класса Pentium и выше;
- тактовая частота процессора не ниже 500 МГц;
- BIOS ЭВМ должна соответствовать спецификации **UEFI BIOS версии не ниже 2.0**;
- требования к объему оперативного запоминающего устройства (оперативной памяти) определяются требованиями ОС, функционирующей в составе данной ЭВМ;
- устройство хранения данных (НЖМД) должно иметь не менее **200 Мбайт** свободного места для установки и функционирования изделия;
- минимальное разрешение экрана видеодисплея ЭВМ должно составлять **800 x 600** пикселей.

2.2 Меры по защите информации и область применения изделия

2.2.1 Изделие может использоваться для защиты информации, обрабатываемой в автоматизированных системах до класса 2А включительно, в государственных информационных системах до класса защищенности К1 включительно, в информационных системах персональных данных до 1 уровня защищенности включительно, в автоматизированных системах управления производственными и технологическими процессами до 1 класса защищенности включительно, в значимых объектах критической информационной инфраструктуры до 1 категории включительно и обеспечения следующих базовых и адаптированных мер защиты информации согласно Приказам ФСТЭК России № 17 от 15.02.2017, № 21 от 23.03.2017, № 31 от 09.08.2018 и № 239 от 25.12.2017 г.:

1) Идентификация и аутентификация пользователей, являющихся работниками оператора (ИАФ.1).

В изделии реализован механизм идентификация и аутентификация пользователей, являющихся работниками оператора с использованием: уникальных учетных записей и паролей, а также персональных электронных идентификаторов. Список поддерживаемых идентификаторов приведен в пункте 1.4 настоящего документа.

2) Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов (ИАФ.3).

В изделии реализована возможность управления уникальными идентификаторами пользователей. Данная функция доступна администратору безопасности после успешного прохождения им процедуры идентификации и аутентификации.

Описание порядка управления идентификаторами пользователей приведено в разделе 8 документа «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 2. Руководство администратора. ГМТК.468269.060РЭ2».

3) Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации (ИАФ.4).

В изделии реализован механизм управления средствами аутентификации пользователей, позволяющий осуществлять хранение в базе данных изделия информации о средствах аутентификации и их сопоставление с пользователями. Указанный механизм осуществляет блокирование загрузки ОС пользователями в случае предъявления ими незарегистрированных (не связанных с каждым конкретным пользователем) средств аутентификации. В случае утраты средств аутентификации доверенная загрузка ОС невозможна для пользователя, утратившего такое средство аутентификации.

Описание порядка управления идентификаторами пользователей приведено в разделе 8 документа «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 2. Руководство администратора. ГМТК.468269.060РЭ2».

4) Защита обратной связи при вводе аутентификационной информации (ИАФ.5).

В изделии реализована защита обратной связи при вводе аутентификационной информации пользователями и администратором безопасности. При вводе паролей и PIN-кодов средств аутентификации вводимая пользователями информация отображается условными знаками «*» или «•» по количеству вводимых символов.

5) Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, за исключением внешних пользователей (УПД.1).

В изделии реализована возможность управления уникальными идентификаторами пользователей. Данная функция доступна администратору безопасности после успешного прохождения им процедуры идентификации и аутентификации.

Описание порядка управления идентификаторами пользователей приведено в разделе 8 документа «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 2. Руководство администратора. ГМТК.468269.060РЭ2».

При использовании изделия все учетные записи пользователей являются внутренними, работа внешних пользователей не предусмотрена в связи с назначением (спецификой применения) изделия.

6) Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы (УПД.4).

В изделии реализовано разделение полномочий администратора безопасности и пользователей. Администратору безопасности доступно управление параметрами и данными изделия после обязательного прохождения идентификации и аутентификации. Пользователи не имеют полномочий для управления параметрами и данными изделия, после прохождения идентификации и аутентификации им доступна только доверенная загрузка ОС (в случае отсутствия ошибок контроля целостности).

7) Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы (УПД.5).

В изделии реализованы следующие роли безопасности: администратор безопасности (встроенная учетная запись) и пользователи. Удаление встроенной учетной записи администратора безопасности исключено.

Выбранная модель ролей безопасности исключает возможность управления параметрами и данными изделия обычными пользователями.

8) Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) (УПД.6).

В изделии реализован механизм ограничения неуспешных попыток входа пользователей и администратора безопасности. Количество попыток входа устанавливается в пределах от 1 до 8 попыток администратором безопасности после его идентификации и аутентификации.

После исчерпания попыток идентификации и аутентификации пользователем его дальнейший доступ в систему блокируется, при этом в зависимости от установленной политики безопасности блокируется учетная запись конкретного пользователя или всех пользователей.

9) Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы (УПД.9).

В изделии в один момент времени возможна работа администратора безопасности (управление параметрами и данными изделия), либо идентификация и аутентификация пользователей и последующая доверенная загрузка ими ОС.

10) Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу (УПД.10).

В изделии реализовано блокирование доступа пользователей после истечения времени на идентификацию и аутентификацию. После истечения времени идентификации и аутентификации пользователей возможна перезагрузка или выключение средства вычислительной техники.

Интервал времени идентификации и аутентификации пользователей задается в пределах от 1 до 30 минут администратором безопасности после его идентификации и аутентификации.

11) Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации (УПД.11).

В изделии запрещены любые действия администратора безопасности и пользователей до их успешной идентификации и аутентификации.

12) Обеспечение доверенной загрузки средств вычислительной техники (УПД.17).

Основное назначение изделия.

13) Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации (ОЦЛ.1).

Изделие реализует контроль целостности объектов (файлов) загружаемой ОС, данных пользователя, каталогов, объектов реестра ОС семейства Microsoft Windows, аппаратных устройств СВТ, загрузочных секторов устройств хранения данных, переменных и драйверов среды UEFI, таблиц ACPI и SMBIOS, журналов транзакций файловых систем NTFS, EXT3, EXT4.

В изделии реализован механизм контроля целостности собственного встроенного программного обеспечения.

14) Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций (ОЦЛ.3).

В изделии реализован механизм автоматического восстановления собственного программного обеспечения при возникновении нештатных ситуаций из резервного хранилища изделия.

2.3 Указания по эксплуатации

2.3.1 Установка изделия должна осуществляться уполномоченным лицом, ответственным за безопасность и эксплуатацию изделия на местах пользователей.

2.3.2 Перед началом использования необходимо ознакомиться с эксплуатационной документацией, входящей в комплект поставки изделия.

2.3.3 Установка изделия на ЭВМ должна производиться в соответствии с документом «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 1. Руководство по установке. ГМТК.468269.060РЭ1».

2.3.4 Установка и эксплуатация изделия должна выполняться только с действующей лицензией на использование, входящей в комплект поставки изделия. Не допускается эксплуатация изделия после истечения срока действия лицензии на использование. Изделие не выполняет функции защиты после истечения срока действия лицензии на использование.

2.3.5 Настройка параметров изделия должна осуществляться в соответствии с документами «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 2. Руководство администратора. ГМТК.468269.060РЭ2» и «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 3. Руководство администратора Linux/Windows. ГМТК.468269.060РЭ3».

2.3.6 Работа пользователей должна осуществляться в соответствии с документом «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 4. Руководство пользователя. ГМТК.468269.060РЭ4».

2.3.7 Восстановление работоспособности изделия после сбоев должно осуществляться в соответствии с документом «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 5. Руководство по безопасному восстановлению. ГМТК.468269.060РЭ5».

2.3.8 Для обеспечения надежной эксплуатации ЭВМ должна иметь минимальным состав технических и программных средств и должна быть произведена первоначальная настройка параметров BIOS Setup.

2.3.9 При создании автоматизированных рабочих мест с использованием изделия обязательна проверка его совместимости и ЭВМ, в составе которого предполагается его использование.

2.3.10 Установка изделия должна осуществляться на ЭВМ защищаемой локальной вычислительной сети, расположенные в контролируемой зоне.

2.3.11 Контроль целостности исполняемых программных модулей на эксплуатируемой ЭВМ во время сеанса работы пользователя, их надежное восстановление из резервных копий и очистка оперативной памяти ЭВМ после завершения процессов должны обеспечиваться сертифицированными средствами защиты информации от несанкционированного доступа.

2.3.12 АБ должен периодически проверять наличие обновлений ОС на официальном сайте разработчика и устанавливать их на эксплуатируемую ЭВМ.

2.3.13 После завершения установки и настройки изделия должна быть приняты организационно-технические меры, исключающие бесконтрольный доступ к изделию и техническим средствам ЭВМ.

2.3.14 После установки изделия на ЭВМ АБ должен установить пароль для входа в BIOS Setup.

2.3.15 АБ запрещается обновлять (модифицировать) ПО UEFI BIOS ЭВМ после установки изделия.

2.3.16 Запрещается использование режимов энергопотребления ЭВМ «Standby» и «Hibernate» при эксплуатации изделия.

2.3.17 Для обеспечения максимальной эффективности использования изделия в составе ЭВМ необходимо обеспечить обязательное выполнение следующих условий эксплуатации:

- обеспечение физической сохранности (целостности) ЭВМ, наличие физической охраны помещения, в котором эксплуатируется ЭВМ и исключение возможности несанкционированного доступа к ЭВМ посторонних лиц;
- хранение в секрете идентификаторов (имен), паролей (кодов), а также PIN-кодов АНП АБ и пользователей;
- периодическая смена паролей и PIN-кодов АНП пользователей и АБ.

3 Описание задачи

3.1 Основной задачей изделия является задача по предотвращению несанкционированного доступа к программным и техническим ресурсам ЭВМ на этапе до загрузки ОС. Для выполнения основной задачи требуется решение следующих задач:

- проверка подлинности пользователя при помощи обязательных процедур идентификации и аутентификации;
- контроль целостности пользовательских файлов, нарушение которых критично для их владельцев;
- контроль завершенности транзакций журналов файловых систем;
- контроль целостности системных файлов и объектов реестра ОС семейства Microsoft Windows;
- контроль параметров среды UEFI;
- контроль загрузочных секторов устройств хранения данных;
- контроль за аппаратной конфигурацией ЭВМ, на которой проводится доверенная загрузка ОС;
- контроль целостности собственного ПО СДЗ;
- предотвращение доступа пользователей до загрузки ОС в случае обнаружения ошибок контроля целостности аппаратной и/или программной конфигурации ЭВМ;
- журналирование основных действий пользователей и администратора безопасности изделия в процессе доверенной загрузки ОС.

3.2 Для решения задачи доверенной загрузки ОС в ПО изделия реализованы следующие основные программные модули:

- ядро СДЗ, реализующее решение указанных в пункте 3.1 задач;
- модуль псевдографического интерфейса для управления параметрами в среде UEFI;
- модуль графического интерфейса для управления параметрами изделия в среде ОС Linux;
- модуль графического интерфейса для управления параметрами изделия в среде ОС Windows.

3.3 Результатом решения задач является обеспечение доверенной загрузки пользователем разрешенной ОС.

4 Входные и выходные данные

4.1 Входными данными являются:

- идентификационная и/или аутентификационная информация пользователей (пароли, АНП и PIN-коды АНП);
- параметры аппаратной конфигурации ЭВМ;
- перечень ОС, установленных на ЭВМ.
- объекты, подлежащие контролю целостности.

Результаты обработки входных данных записываются в базу данных изделия.

4.2 Выходными данными являются:

- список зарегистрированных пользователей и соответствующие им идентификационные и/или аутентификационные данные;
- список соответствия «пользователь» - «доверенные к загрузке ОС»;
- список установленных на контроль целостности объектов файловой системы, каталогов, объектов реестра ОС семейства Microsoft Windows, аппаратных устройств ЭВМ, загрузочных секторов устройств хранения данных, переменных и драйверов среды UEFI, таблиц ACPI и SMBIOS, журналов завершенности транзакций файловых систем NTFS, EXT3, EXT4;
- системный журнал, содержащий основные сведения о действиях пользователей и администратора безопасности до доверенной загрузки ОС.

Результаты обработки выходных данных записываются в базу данных изделия.

4.3 При выявлении нарушений контроля целостности аппаратной и программной конфигурации ЭВМ выходными данными также являются информационные сообщения о нарушениях, выводимые на экран ЭВМ АБ.

Перечень сокращений

ACPI	–	Advanced Configuration and Power Interface (усовершенствованный интерфейс управления конфигурацией и питанием)
BIOS	–	Basic Input Output System (базовая система ввода-вывода)
EXT3, EXT4	–	Extended File System (расширенная файловая система)
FAT32	–	File Allocation Table (таблица размещения файлов)
GRUB	–	Grand Unified Bootloader (загрузчик операционной системы от проекта GNU)
LILO	–	LInux Loader (стандартный загрузчик для Linux и BSD-систем)
LSB	–	Linux Standard Base (совместный проект семейства операционных систем, основанных на Linux)
MBR	–	Master Boot Record (главная загрузочная запись)
NTFS	–	New Technology File System (файловая система новой технологии)
PIN	–	Personal Identification Number (личный идентификационный номер)
PKI	–	Public Key Infrastructure (инфраструктура открытых ключей)
SMBIOS	–	System Management BIOS (системное управление BIOS)
UDF	–	Universal Disk Format (универсальный дисковый формат)
UEFI	–	Unified Extensible Firmware Interface (интерфейс управляющими низкоуровневыми функциями оборудования)
USB	–	Universal Serial Bus (последовательный интерфейс для подключения периферийных устройств к вычислительной технике)
АБ	–	администратор безопасности
АНП	–	аутентификационный носитель пользователя
АО	–	акционерное общество
ГОСТ	–	государственный стандарт
ЗАО	–	закрытое акционерное общество

ИАФ	–	идентификация и аутентификация
КИ	–	конфиденциальная информация
НЖМД	–	накопитель на жестких магнитных дисках
ОС	–	операционная система
ОЦЛ	–	обеспечение целостности
ПО	–	программное обеспечение
РД	–	руководящий документ
С	–	секретно
СВТ	–	средство вычислительной техники
СДЗ	–	средство доверенной загрузки
УПД	–	управление правами доступа
ФСТЭК России	–	Федеральная служба по техническому и экспортному контролю России
ЭВМ	–	электронно-вычислительная машина
ЭЦП	–	электронная цифровая подпись