ООО «ВАЛИДАТА»

УТВЕРЖДЕН
ВАМБ.00060-06–ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ «ВАЛИДАТА CSP» ВЕРСИЯ 6

КОНТРОЛЬ ЦЕЛОСТНОСТИ

Руководство администратора информационной безопасности

ВАМБ.00060-06 93 02

2020

Аннотация

В настоящем документе описаны требования к организации процедуры контроля целостности программного обеспечения (ПО) систем криптографической защиты информации (СКЗИ) и системного ПО (допустимый инструментарий, виды контроля и порядок контроля целостности), а также порядок действий при обнаружении нарушения целостности ПО.

Данный документ предназначен для лиц, ответственных за контроль целостности ПО в процессе эксплуатации СКЗИ.

Содержание

1 ИНСТРУМЕНТАРИЙ КОНТРОЛЯ ЦЕЛОСТНОСТИ И ОБЪЕКТЫ КОНТРОЛЯ

1.1 Программа hashfile.exe

Программа контроля целостности (далее - программа **hashfile.exe**) выполняет расчет и проверку значений хэш-функции для заданного списка контролируемых файлов. Данная программа входит в состав программного комплекса ВАМБ.00060-06 «СКЗИ «Валидата CSP» версия 6» (далее — СКЗИ «Валидата CSP»). Описание порядка работы с программой **hashfile.exe** приведено в документе ВАМБ.00060-06 92 01 «СКЗИ «Валидата CSP» версия 6. Программа контроля целостности. Руководство пользователя».

Программа **hashfile.exe** выполняет хэширование данных в соответствии с ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования».

1.2 Программно-аппаратные СЗИ ОТ НСД

Применительно к СКЗИ, обеспечивающим защиту по уровню КС2 и КС3, обязательным является требование использования для контроля целостности программной среды сертифицированного ФСБ России программно-аппаратного средства защиты от несанкционированного доступа (ПА СЗИ от НСД), реализующего на аппаратном уровне запрет загрузки операционной системы с внешних носителей и контроль целостности ПО. Перечень разрешенных к использованию СЗИ от НСД указан в документе ВАМБ.00060-06 30 01 «СКЗИ «Валидата CSP» версия 6. Формуляр».

Установка и настройка ПА СЗИ от НСД выполняется согласно положениям соответствующих эксплуатационных документов. Настройка установленных на конкретном рабочем месте ПА СЗИ должна обеспечить санкционированный доступ пользователей рабочего места к назначенным для них ресурсам и исключать возможность их вмешательства в процессы загрузки операционной системы (ОС) и прикладного ПО и процесс проверки целостности программной среды.

Контроль целостности с использованием ПА СЗИ от НСД должен осуществляться до перехода средств вычислительной техники, на которых реализовано СКЗИ, в рабочее состояние (до загрузки ОС). Списки файлов, подлежащих контролю целостности с использованием ПА СЗИ от НСД, должны содержать файлы ПО самого ПА СЗИ от НСД, а также исполняемый файл программы **hashfile.exe** и эталон верификации (при использовании программы **hashfile.exe** для контроля целостности).

Примечания.

1. Эталон верификации - один из следующих объектов:

*– создаваемый программой **hashfile.exe** файл, содержащий список файлов, подлежащих контролю целостности, и значение хэш-функции для каждого файла из данного списка;*

– ветка реестра ОС Windows, содержащая перечень файлов, подлежащих контролю целостности, и значения хэш-функции для каждого файла из данного перечня.

*2. В случае необходимости организации контроля целостности с использованием реестра ОС Windows средствами программы **hashfile.exe** необходимо добавить в реестр хэш-значения всех модулей, подлежащих контролю целостности.*

При хранении эталона верификации в реестре ОС Windows, должен быть организован контроль целостности соответствующей ветки реестра с помощью ПА СЗИ от НСД, а также приняты организационно-технические меры, обеспечивающие защиту от несанкционированного локального и удаленного доступа к реестру ОС.

1.3 Объекты контроля целостности

Контролю целостности подлежат следующие объекты:

- ПО программных средств контроля целостности (программа **hashfile.exe**);
- ПО программно-аппаратных средств контроля целостности;
- ПО средств создания замкнутой программной среды;
- ПО СКЗИ;
- Системное ПО;
- Эталон верификации.

2 ОБЩИЙ ПОРЯДОК ПРИМЕНЕНИЯ СРЕДСТВ КОНТРОЛЯ ЦЕЛОСТНОСТИ К ОБЪЕКТАМ КОНТРОЛЯ

Для контроля целостности допускается применять один из следующих подходов:

1. В качестве основного средства контроля целостности используется программа **hashfile.exe**, целостность программы **hashfile.exe** и эталона верификации при этом обеспечивается либо средствами СЗИ от НСД, либо организационно-техническими мерами, такими как финализированная запись этих объектов на отчуждаемый носитель (CD- или DVD-диск), правила обращения с которым соответствуют правилам обращения с ключевыми носителями.

2. В качестве основного средства контроля целостности используется СЗИ от НСД, а программа **hashfile.exe** при необходимости используется в качестве дополнительного средства контроля. Целостность исполняемого файла программы **hashfile.exe** и эталона верификации при этом обеспечивается средствами СЗИ от НСД.

Рассмотрим более подробно каждый из описанных выше подходов.

2.1 Использование утилиты hashfile.exe в качестве основного средства контроля целостности

В настоящем разделе описаны способы организации контроля целостности при использовании в качестве основного средства контроля целостности утилиты **hashfile.exe** в зависимости от наличия в эксплуатирующей организации ПА СЗИ от НСД.

2.1.1 Использование утилиты hashfile.exe без ПА СЗИ от НСД

В случае, если основным средством контроля целостности является программа **hashfile.exe** и отсутствуют ПА СЗИ от НСД, сертифицированные по требованиям ФСБ России, необходимо руководствоваться следующим порядком применения средств контроля целостности:

– контроль целостности ПО СКЗИ и системного ПО выполняется с использованием программы **hashfile.exe**;

– контроль целостности программы **hashfile.exe** и эталона верификации выполняется с использованием организационно-технических мер, таких, как финализированная запись исполняемого модуля данной программы и эталона верификации на отчуждаемый носитель (CD- или DVD-диск), правила обращения с которым соответствуют правилам обращения с ключевыми носителями. Хранение эталона верификации в реестре ОС Windows в этом случае не допускается.

2.1.2 Использование утилиты hashfile.exe совместно с ПА СЗИ от НСД

В случае, если основным средством контроля целостности является программа **hashfile.exe** и имеются ПА СЗИ от НСД, сертифицированные по требованиям ФСБ России, необходимо руководствоваться следующим порядком применения

средств контроля целостности:

– контроль целостности ПО СКЗИ и системного ПО выполняется с использованием программы **hashfile.exe**;

– контроль целостности программы **hashfile.exe** и эталона верификации выполняется с использованием ПА СЗИ от НСД и/или организационно-технических мер, таких, как финализированная запись исполняемого модуля данной программы и эталона верификации на отчуждаемый носитель (CD- или DVD-диск), правила обращения с которым соответствуют правилам обращения с ключевыми носителями;

– контроль целостности ПО средств создания замкнутой программной среды (при их наличии) выполняется ПА СЗИ от НСД;

– контроль целостности программного обеспечения ПА СЗИ от НСД выполняется с использованием самих этих средств.

2.2 Использование ПА СЗИ от НСД в качестве основного средства контроля целостности

В настоящем разделе описан способ организации контроля целостности при использовании в качестве основного средства контроля целостности ПА СЗИ от НСД, сертифицированных ФСБ России. В этом случае необходимо руководствоваться следующим порядком применения средств контроля целостности:

– контроль целостности ПО СКЗИ, ПО средств создания замкнутой программной среды (при их наличии) и системного ПО выполняется до загрузки ОС средствами ПА СЗИ от НСД;

– контроль целостности программного обеспечения ПА СЗИ от НСД выполняется с использованием самих этих средств.

При использовании в качестве основного средства контроля целостности ПА СЗИ от НСД использование программы **hashfile.exe** для проверки целостности не является обязательным. При этом данную программу необходимо использовать в качестве дополнительного средства контроля целостности в случаях, когда условия эксплуатации СКЗИ не допускают проведение контроля целостности средствами ПА СЗИ от НСД (т.е. перезагрузки ЭВМ) в произвольный момент времени. В иных случаях использование программы **hashfile.exe** в качестве дополнительного средства контроля целостности остается на усмотрение эксплуатирующей организации.

Если программа **hashfile.exe** используется в качестве дополнительного средства контроля целостности, целостность данной программы и эталона верификации необходимо контролировать средствами ПА СЗИ от НСД.

2.3 Рекомендации по организации контроля целостности в зависимости от реализуемого класса защиты и условий эксплуатации СКЗИ

С учетом требуемого уровня защиты допустимый инструментарий для контроля целостности можно обобщить следующим образом:

– для СКЗИ, обеспечивающих защиту по классу КС2 и КС3 (в этом случае

использование ПА СЗИ от НСД является обязательным), контроль целостности осуществляется по схемам, описанным в разделах 2.1.2 или 2.2.

– для СКЗИ, обеспечивающих защиту по классу КС1:

• при отсутствии ПА СЗИ от НСД, сертифицированного по требованиям ФСБ России, используется схема, описанная в разделе 2.1.1;

• при наличии ПА СЗИ от НСД, сертифицированного по требованиям ФСБ России, может использоваться тот же способ контроля целостности, что для СКЗИ, обеспечивающих защиту по классу КС2 и КС3.

Конкретный выбор того или иного средства контроля целостности определяется требуемым классом защиты информации, имеющимися ПА СЗИ от НСД и доступными для реализации организационно-техническими мерами защиты. При этом при выборе того или иного средства контроля целостности в качестве основного дополнительно необходимо руководствоваться следующими требованиями:

1. При организации контроля целостности средств удостоверяющего центра (и средств ЭП, совместно с которыми он функционирует) в качестве основного средства контроля целостности необходимо использовать ПА СЗИ от НСД (см. раздел 2.2).

2. При использовании в качестве основного средства контроля целостности ПА СЗИ от НСД в обязательном порядке должны выполняться требования по контролю правильности работы аппаратных средств ПЭВМ, предписывающие проводить перезагрузку ЭВМ с установленным СКЗИ с периодом не более 72 часов (3-х суток) в связи с тем, что контроль целостности средствами ПА СЗИ от НСД выполняется до загрузки ОС.

3 ВИДЫ КОНТРОЛЯ ЦЕЛОСТНОСТИ

Мероприятия по контролю целостности должны включать в себя следующие виды работ:

– контроль целостности дистрибутивов;

– первичный контроль - контроль целостности, выполняемый при поставке ПО;

– текущий (ежедневный) контроль - контроль целостности, выполняемый в процессе работы с ПО (в начале работы, во время работы или по завершении работы) пользователем или уполномоченным контролирующим лицом;

– периодический (регламентный) контроль - контроль целостности, выполняемый администратором информационной безопасности в соответствии с принятым в эксплуатирующей организации регламентом.

3.1 Контроль целостности дистрибутивов СКЗИ

3.1.1 Первичный контроль

Первичный контроль дистрибутива СКЗИ выполняется перед установкой СКЗИ на ЭВМ системным администратором (лицом, выполняющим установку СКЗИ).

Для СКЗИ, поставляемом на передаточном носителе в виде компакт-диска, используется программа **hashfile.exe** и эталон верификации установочных файлов (они же - списки контроля целостности дистрибутива), помещаемые на дистрибутивном диске.

Для СКЗИ, поставляемом на передаточном носителе в электронном виде и подписанном ЭП, для проведения первичного контроля используется СКЗИ «Валидата CSP» или иное сертифицированное средство ЭП.

Эталонные дистрибутивы с подтвержденной целостностью должны храниться в условиях, исключающих возможность подмены установочных файлов и файлов верификации.

3.1.2 Периодический контроль

Периодический контроль целостности дистрибутивов выполняется лицом, ответственным за учет и хранение программного обеспечения, тем же образом, что и первичный контроль, с периодом не более 30 дней.

3.2 Первичный контроль

СКЗИ устанавливается на соответствующие технические средства в соответствии с его руководством по установке только после успешной проверки целостности дистрибутива СКЗИ.

В случае использования в качестве основного средства контроля целостности ПА СЗИ от НСД, необходимо внести подлежащие контролю целостности файлы в список файлов, контролируемых соответствующим СЗИ от НСД.

При использовании программы **hashfile.exe** для контроля целостности (как в качестве основного, так и дополнительного средства контроля) на выделенном (эталонном) автоматизированном рабочем месте (АРМ) сотрудником подразде-

ления информационной безопасности или администратором информационной безопасности с помощью программы **hashfile.exe** рассчитываются контрольные (первичные) значения хэш-функций (далее - эталон верификации):

– для всех файлов прикладного ПО АРМ (не изменяемых в процессе эксплуатации);

– для всех файлов СКЗИ и файлов ОС, подлежащих контролю целостности.

Примечание - При наличии однотипных АРМ, работающих под управлением разных ОС, первичные значения хэш-функций для контролируемых файлов ОС, под управлением которой работает АРМ, рассчитываются для каждой конкретной ОС (с учетом установленных ее обновлений) и в дальнейшем используются совместно с файлами верификации эталонного АРМ (эталоном верификации).

Эталон верификации в дальнейшем используется для контроля целостности ПО всех АРМ.

Также рекомендуется создать копии эталона верификации на отчуждаемом носителе (либо в печатном виде) и хранить их в защищенном от изменения виде (для возможности контроля подлинности эталона верификации со стороны администратора информационной безопасности).

При установке обновлений ОС могут быть изменены файлы ПО ОС, входящие в среду функционирования СКЗИ. В этом случае потребуется обновление эталона верификации. Поэтому при установке обновлений ОС необходимо руководствоваться следующим порядком действий:

а) Перед установкой обновлений проверить целостность системного ПО с использованием текущего эталона верификации (при использовании программы **hashfile.exe**) или перезагрузить ЭВМ (при использовании для контроля целостности только ПА СЗИ от НСД);

б) Выполнить установку обновлений ОС и перезагрузить ЭВМ;

Примечание – В случае использования ОС Windows 10, Windows Server 2016 и Windows Server 2019 после установки обновлений необходимо выполнить действия, указанные в документе ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности»

в) Запустить проверку целостности системного ПО с использованием текущего эталона верификации. Если проверка целостности завершилась успешно, обновление эталона верификации не требуется. В противном случае необходимо обновить эталон верификации, заново рассчитав значения хэш-функций для всех файлов системного ПО, и/или обновить контрольные характеристики измененных файлов в списке файлов, контролируемых с помощью ПА СЗИ от НСД.

3.3 Текущий контроль

Текущий контроль целостности ПО в обязательном порядке выполняется пользователем на своем рабочем месте перед началом работы с СКЗИ и при необходимости в любой произвольный момент времени.

Если в качестве основного средства контроля целостности используется программа **hashfile.exe**, для проведения текущего контроля необходимо использовать данную программу и эталон верификации. Вызов программы **hashfile.exe**

для контроля целостности ПО должен производиться до запуска прикладных задач пользователя (до первого обращения к любому исполняемому модулю СКЗИ).

Если в качестве основного средства контроля целостности используются ПА СЗИ от НСД, текущий контроль целостности, выполняемый перед началом работы с СКЗИ, выполняется до загрузки ОС средствами ПА СЗИ от НСД. При необходимости проведения контроля целостности в произвольный момент времени необходимо либо выполнить перезагрузку ЭВМ, либо использовать программу **hashfile.exe** и эталон верификации (программа **hashfile.exe** в этом случае используется в качестве дополнительного средства контроля, см. раздел 2.2).

3.4 Регламентный контроль

Если в качестве основного средства контроля целостности используется программа **hashfile.exe**, администратор информационной безопасности должен периодически (с периодом не более 30 дней) проводить полный контроль целостности ПО СКЗИ и системного ПО на всех рабочих местах с помощью программы **hashfile.exe** и эталона верификации. Проверка целостности в ходе регламентного контроля должна осуществляться до первого обращения к любому исполняемому модулю СКЗИ или прикладного ПО.

Примечание - Если ПЭВМ с установленным СКЗИ не используется (выключена) более 30 дней, проводить регламентный контроль не требуется. При этом важно обеспечить надлежащую защиту от несанкционированного использования ПЭВМ. Перед началом боевого использования данной ПЭВМ необходимо провести её регламентный контроль, а последующие периоды регламентного контроля отсчитывать с этого момента.

Если в качестве основного средства контроля целостности используются ПА СЗИ от НСД, отдельные мероприятия по организации регламентного контроля не проводятся: выполнение требований документа ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности», предписывающих проводить перезагрузку работающей ПЭВМ с установленным СКЗИ с периодом не более 72 часов (3 суток), обеспечивает проведение контроля целостности ПО СКЗИ и системного ПО средствами ПА СЗИ от НСД с таким же периодом, так как проверка целостности средствами ПА СЗИ от НСД выполняется при каждом включении ПЭВМ или её перезагрузке.

4 ДЕЙСТВИЯ ПРИ ОБНАРУЖЕНИИ НАРУШЕНИЯ ЦЕЛОСТНОСТИ

4.1 Общие требования

При обнаружении нарушения целостности ПО прежде всего необходимо установить причину нарушения целостности.

Если причиной нарушения целостности ПО является аппаратный сбой, необходимо выполнить переустановку ОС, ПО СКЗИ и произвести восстановление баз данных (при их наличии) с использованием резервных копий. Если причиной является программный сбой, следует также переустановить ОС (если нарушена целостность файлов среды функционирования криптосредства (СФК)) и ПО СКЗИ (если нарушена целостность файлов ПО СКЗИ) и также восстановить базы данных.

Если причиной является вирусная атака, необходимо установить, каким путем было заражено ПО, кем и какие требования правил пользования ПО СКЗИ были нарушены, а также проверить актуальность используемого антивирусного ПО и, при необходимости, обновить его. Далее необходимо оценить возможные опасные последствия вирусной атаки (возможность утечки информации ограниченного доступа, искажение алгоритмов функционирования ПО СКЗИ, компрометация ключей ЭП). Рекомендуется, при обнаружении вирусной атаки, выполнять переустановку ОС и ПО СКЗИ, а также восстановление баз данных.

4.2 Восстановление целостности ПО

Для создания резервных копий СКЗИ рекомендуется использовать **Мастер архивации** ОС Windows - утилиту типа **Backup**. Пользование **Мастером архивации** во всех ОС Windows примерно одинаково. Подробные правила пользования сервисом архивации можно найти в системной справочной службе. Кроме того, сам **Мастер архивации** работает в интерактивном режиме с выдачей пользователю подробных инструкций.

Рекомендуется задавать следующие установки и параметры архивации:

– использовать возможность выбора объектов для архивации;

– при задании типа архивации, определяющего стратегию резервного копирования, исходить из необходимости быстрого, надежного и максимально полного восстановления исходных объектов архивации. Стандартная стратегия архивации - один или два раза в неделю проводить обычную архивацию, а между ней один или два раза в день добавочную или разностную. Поскольку при разностной архивации состояние архивного бита не изменяется, в каждую разностную архивацию включаются все новые файлы, а также файлы, изменившиеся с последней обычной архивации. Чтобы восстановить архивируемые данные в случае разностных архиваций, необходимо восстановить последний обычный и последний разностный архив. По этой причине можно отдать предпочтение разностной архивации;

– при задании способа архивации задавать проверку данных после архивации;

– при задании параметров архивации использовать добавление нового архива к уже существующим (для гарантии сохранения всей истории архивирования);

– не отключать теневое копирование;

– предоставить право архивации только администратору или оператору архива;

– установить флажок "***Разрешать доступ к данным только владельцу и администратору***", чтобы ограничить доступ к создаваемому архиву. В будущем все данные, дописываемые к архиву, будут попадать под это ограничение доступа;

– при задании периодичности архивирования использовать задание расписания архивирования, учитывающее расписание использования программы.

Кроме того, рекомендуется выполнять следующие правила:

– осуществлять копирование на внешний носитель;

– хранить копии внешнего носителя в безопасном месте;

– разработать и проверить на практике систему архивации и восстановления;

– составить еженедельный график пробного восстановления данных. Периодически выполнить пробное восстановление для проверки правильности архивации файлов. Пробное восстановление может помочь обнаружить неполадки оборудования, незаметные при программной проверке;

– в сетях с минимальной или средней защитой наделить правами архивации одного пользователя, а правами восстановления - другого;

– обучить сотрудников с правами на восстановление выполнять все задачи восстановления в случае отсутствия администратора;

– в сетях с высокой защитой восстановление файлов должно выполняться только администраторами;

– архивировать тома целиком. Архивация всего тома обеспечивает готовность к негативным событиям типа поломки диска. Операция восстановления всего тома за один прием является более эффективной;

– для каждой архивации создать и печатать журналы архивации. Следить за журналами архивации и убедиться в том, что архивация была успешно завершена. Для упрощения нахождения каких-либо файлов хранить книгу журналов. Журналы архивации, которые можно напечатать или просмотреть в любом текстовом редакторе, полезны при восстановлении данных. Кроме того, если носитель, содержащий каталог архива, поврежден, напечатанный журнал поможет найти требуемый файл;

– обеспечить безопасность устройств хранения данных и носителей архива. Восстановление данных с утерянного носителя возможно каким-либо пользователем на другом сервере, администратором которого он является.

4.3 Список резервируемых файлов

Список файлов ПО СКЗИ, подлежащих резервированию, совпадает со списком файлов, подлежащих контролю целостности.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АРМ	Автоматизированное рабочее место
КЗИ	Криптографическая защита информации
ОС	Операционная система (Operating System)
ПА СЗИ от НСД	Программно-аппаратные средства защиты информации от несанкционированного доступа
ПО	Программное обеспечение
СКЗИ	Средство криптографической защиты информации

Лист регистрации изменений

Номера листов (страниц)					Всего листов (страниц) в докум	№ документа	Входящий № сопроводительного докум и дата	Подп	Дата
Изм	изменённых	заменённых	новых	аннулированных					