

Специальный съемный носитель как среда передачи журналов средств доверенной загрузки

¹ Д. А. Эпиктетов; ^{1,2,3} А. А. Алтухов

¹ Московский физико-технический институт (государственный университет), г. Долгопрудный, Московская область, Россия

² Закрытое акционерное общество "ОКБ САПР", Москва, Россия

³ Национальный исследовательский ядерный университет "МИФИ", Москва, Россия

Рассматривается способ сбора журналов средств доверенной загрузки (СДЗ), основанный на использовании специального носителя информации и особо организованной архитектуре взаимодействия СДЗ со средой передачи и обработки журналов. Предложенный способ позволяет организовать полуавтоматический сбор журналов, исключая необходимость интегрировать СДЗ в специальные системы по сбору журналов или предъявлять дополнительные требования к информационной системе, обеспечивающей передачу и сбор журналов.

Ключевые слова: сбор журналов, регистрация событий, журнал работы СДЗ, USB-устройство с управляемым доступом.

Неотъемлемой составляющей работы современных информационных систем является аудит, т. е. процесс записи информации о происходящих событиях в какое-либо хранилище (журнал). В современных операционных системах (ОС) для этого имеются встроенные средства (например, демон *rsyslogd* в семействе *GNU/Linux* и "Журнал событий" в *Windows*). Они позволяют сохранять информацию о происходящих событиях от различных источников в одном месте, предоставляют приложениям программный интерфейс (API) для записи и чтения журнала, а также предоставляют доступ к журналу пользователю. Используя дополнительное программное обеспечение, можно обеспечить передачу данных, предназначенных для внесения в журнал, по сети.

При расследовании инцидентов информационной безопасности (ИБ) одним из ключевых моментов является работа с журналами операционных систем, систем обнаружения вторжений, антивирусов и других систем безопасности [1, 2].

Для банковских систем должно быть реализовано ведение журналов действия и операций автоматизированных рабочих мест, серверного и сете-

вого оборудования, межсетевых экранов и АБС с целью их использования при реагировании на инциденты ИБ [3]. Для защиты информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (ГИС), и для защиты персональных данных при их обработке в информационных системах персональных данных (ИСПДн) должна обеспечиваться регистрация событий безопасности, что подразумевает сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе (ИС), а также возможность просмотра и анализа информации о таких событиях и реагирование на них [4, 5].

В автоматизированных системах управления технологическим процессом (АСУ ТП), где цена ошибки может быть неизмеримо велика, крайне важно иметь точную информацию о том, что именно происходило в каждый момент времени, чтобы в случае сбоя в работе имелась возможность как можно быстрее выявить неисправную составляющую системы и причину, вызвавшую неправильное функционирование, и как можно быстрее восстановить работоспособность. Обработка журналов средств защиты информации, применяемых в таких системах, может помочь оперативно выявить вторжения или их попытки и отреагировать на них должным образом, возможно предотвратив непоправимые катастрофические последствия [6].

Информация, содержащаяся в журналах, нуждается в защите (как уже говорилось это подтверждают и нормативные документы). Это могут

Эпиктетов Денис Андреевич, студент 3-го курса.

E-mail: d.epiktetov@okbsapr.ru

Алтухов Андрей Андреевич, программист 1-й категории группы программирования ПО СЗИ, ассистент, аспирант.

E-mail: altuhov@okbsapr.ru

Статья поступила в редакцию 5 июня 2017 г.

© Эпиктетов Д. А., Алтухов А. А., 2017

быть, например, журналы средств доверенной загрузки (СДЗ) [7]. В данной статье будет предложено решение задачи автоматизации сбора таких журналов на примере модуля доверенной загрузки "Аккорд-АМДЗ". Он включает в себя подсистему регистрации событий, журналы безопасности сохраняются в энергонезависимую память [8]. Однако в некоторых случаях очень важно иметь к ним оперативный доступ, что невозможно, если журналы каждого экземпляра АМДЗ хранятся только локально, т. е. только в памяти соответствующего АМДЗ. К тому же рано или поздно она может закончиться. В результате возникает необходимость в средстве сбора подобных журналов для обработки, анализа и хранения. Для повышения уровня безопасности ИС журналы нужно хранить в изолированном хранилище, физически отделённом от технических средств, входящих в состав ИС [9]. Кроме того, необходимо обеспечить быстрый и удобный доступ к ним.

Для понимания проблем, возникающих при попытке организовать автоматизированный сбор журналов СДЗ, необходимо разобрать формальную модель, лежащую в основе большинства средств сбора журналов.

Наиболее популярный подход по организации сбора и обработки данных в корпоративных или государственных системах — это клиент-серверный подход.

В самом общем случае хранение и обработка журналов должны происходить в некотором узле обработки данных. Будем называть его центральным хранилищем журналов (ЦХЖ). Обычно сбор журналов реализуется с помощью передачи данных по сети. Передача данных может производиться с помощью самых различных сетевых протоколов, например с помощью *NetBIOS*, *RPC*, *TFTP*, *FTP*, *SSH*. Безопасность передаваемых данных может быть обеспечена с помощью самих сетевых протоколов или защищенных виртуальных каналов, например VPN. Естественно, доверенная среда является необходимым условием безопасной обработки журналов как на стороне клиентской, так и на стороне серверной части. Клиентское и серверное ПО, собирающие журналы, должны работать в доверенной среде. Возможны и менее стандартные подходы к организации процесса передачи данных с использованием специализированных аппаратных средств [10].

Следует отметить, что даже если сбор данных происходит с помощью отчуждаемых носителей с каждой локальной станции без какой-либо автоматизации, то и в этом случае есть нечто, выполняющее роль ЦХЖ, например автоматизированное рабочее место (АРМ) администратора информации

онной безопасности (АИБ), где в дальнейшем происходят анализ и обработка журналов.

Разработка средств автоматизированного сбора журналов с ЭВМ, использующих сети передачи данных, является активно развивающейся сферой. В частности, огромное количество *SIEM*-решений, существующих на западном и отечественном рынке, доказывает приведенное утверждение. Интеграция подобных средств сбора журналов в ИС заключается в установке и настройке специализированного серверного ПО, которое занимается обработкой данных, собранных со всех клиентских ЭВМ, а также в установке на каждую ЭВМ, с которой нужно собирать журналы, клиентской части ПО. При интеграции средства сбора журналов во все вычислительные узлы могут возникать проблемы.

Одна из проблем — это невозможность установить клиентскую часть ПО на специализированную ЭВМ. Не все компоненты ИС являются обычными ПК. Это могут быть и специализированные ЭВМ, использующие непопулярные архитектуры, которые не поддерживаются популярными средствами сбора журналов, либо ЭВМ имеющие особую структуру и не позволяющие устанавливать дополнительное ПО без участия их разработчика или поставщика. Такие ЭВМ активно применяются в сфере АСУ ТП. Интеграция подобной ЭВМ и средства сбора журналов приводит к необходимости дополнительных работ как разработчика средства сбора журналов, так и разработчика специализированного СВТ.

Еще одна проблема связана с невозможностью использовать сеть для передачи данных средством сбора журналов. Такая ситуация может возникать, если клиентская ЭВМ не может быть подключена к сети из-за технических ограничений или по соображениям безопасности. Требования безопасности также могут не позволять передачу журналов по сети, что приводит к необходимости найти альтернативный подход, например использовать специализированную физически изолированную сеть.

Средство доверенной загрузки является реализацией резидентного компонента безопасности. Из требований, предъявляемых к РКБ, следует невозможность штатно установить дополнительное ПО в состав СДЗ, что приводит к возникновению проблемы интеграции СДЗ в существующие решения сбора журналов. Единственным возможным решением является расширение функциональности СДЗ за пределы функций обеспечения доверенной загрузки. Здесь возможны разные варианты.

Один из вариантов — это обеспечить поддержку существующих решений сбора журналов и добавить их в состав функциональности СДЗ. Одна-

ко какое из многочисленных средств следует поддерживать? Выгодно поддерживать все возможные решения, но это нереально. Можно поддерживать только некоторые из них, но в таком случае возможность использования функции сбора журналов СДЗ будет зависеть от используемого в ИС средства сбора журналов.

Можно создать свое средство сбора журналов и обеспечить интеграцию с другими существующими решениями. Такой вариант позволяет вынести максимум функциональности, связанной с обработкой и передачей данных из СДЗ, и перенести в другой продукт. Таким способом можно обеспечить модульность архитектуры и не перегружать СДЗ излишней функциональностью. С другой стороны, придется сталкиваться с теми же проблемами, с которыми сталкиваются разработчики средств автоматизированного сбора журналов.

Следует отметить, что в случае поддержки решений по сбору журналов в составе СДЗ возникает целая область, которую нужно исследовать, — уязвимости, связанные с сетевым взаимодействием [11], безопасность используемых протоколов, а также среды передачи данных, что расширяет функциональность и задачи, которые ставятся перед СДЗ. В этом случае реализация СДЗ также будет включать и функциональность, связанную с безопасной передачей данных, что не имеет прямого отношения к основной функциональности продукта.

Можно пойти другим путем — осуществлять сбор информации на ЦХЖ вручную с каждого экземпляра СДЗ (например, с помощью некоторого съемного носителя) [12], однако в случае большого их количества работа администратора ИБ будет трудоёмкой. Следует отметить, что данный подход является работоспособным, даже если вычислительные узлы не подключены к сети передачи данных.

Средство сбора журналов СДЗ должно обеспечить:

- поддержку максимально возможных средств сбора и обработки журналов;
- максимальное уменьшение трудоёмкости работы АИБа;
- добавление минимума новой функциональности в СДЗ;
- возможность интеграции и модификации в соответствии с конечной архитектурой ИС.

Предлагаемый далее способ реализации сбора журналов объединяет два подхода: создание своего средства сбора журналов и сбор журналов "локально" с использованием внешнего носителя. Создание специализированного средства сбора жур-

налов избавит от необходимости реализовывать функциональность взаимодействия с другими системами сбора журналов в СДЗ. Идея сбора журналов с помощью специального отчуждаемого носителя позволит создать свою дополнительную промежуточную среду передачи данных между СДЗ и средой передачи данных ИС.

Для решения проблем интеграции предлагается использовать простую и защищенную промежуточную среду передачи данных, с которой СДЗ может взаимодействовать и которая легко встраивается в проектируемую ИС. В общем случае промежуточная среда обеспечит безопасную передачу журналов от СДЗ до некоторого устройства синхронизации журналов (УСЖ), задача которого — передать полученные журналы в ЦХЖ. Организация процесса передачи данных от УСЖ до ЦХЖ выходит за рамки функционирования СДЗ и в каждом конкретном случае может происходить по-своему с учетом особенностей проектируемой системы. Необходимо предложить вариант реализации промежуточной среды, которую можно использовать на участке от СДЗ до УСЖ, и описать взаимодействие СДЗ и УСЖ с данной средой. Данная среда передачи и взаимодействия не должны зависеть от параметров ИС, по которой данные будут передаваться в ЦХЖ.

Каждый пользователь ЭВМ, на которой установлено СДЗ, будет самостоятельно регулярно переносить журналы в УСЖ для последующей передачи в ЦХЖ. Это сильно облегчает работу администратора ИБ, однако не исключает некоторых угроз, связанных со средой передач: журналы определенное время пребывают на съемном носителе, находящемся в руках пользователя. Возможны потеря носителя, его хищение, даже попытка извлечения или модификации информации, содержащейся на нем, самим пользователем. Однако информация, содержащаяся в журналах аудита, должна быть защищена от несанкционированного доступа и несанкционированного изменения [13]. Доступ к записям аудита и функциям управления механизмами регистрации (аудита) должен предоставляться только уполномоченным должностным лицам [10]. Поэтому необходимо исключить возможность изменения пользователем уже содержащихся на съемном носителе данных, при этом сохранив возможность их добавления.

Все сказанное позволяет сформулировать требования к устройству, с помощью которого будет осуществляться перенос журналов СДЗ (назовем его портативным хранилищем журналов, ПХЖ):

- возможность только добавлять на носитель копии журналов;

- невозможность удалить содержимое архивной копии журнала, содержащейся на носителе, до истечения срока хранения;

- доступность просмотра архивных копий журнала только уполномоченными субъектами;

- большой размер дискового пространства, достаточный для хранения архивных копий журналов;

- изолированность хранилища от технических средств, входящих в состав ИС;

- контроль целостности содержимого архива;

- простая интеграция с системами защиты информации;

- возможность использования хранилища только на компонентах контролируемой ИС [14].

Для выполнения сформированных требований можно использовать USB-устройство с флеш-памятью с управляемым доступом и внешнее ПО (утилиты для сбора, просмотра архивируемых журналов, настройки, контроля работы устройства и библиотеки записи журнала). Устройства со схожей функциональностью существуют (например, "Программно-аппаратный журнал" — один из продуктов линейки "Секрет", выпускаемой ЗАО "ОКБ САПР") [15]. Используя аппаратную часть данного ПАК и доработав программную часть, не составляет труда реализовать ПХЖ.

В СДЗ "Аккорд-АМДЗ" необходимо добавить функциональность, поддерживающую возможность экспорта журналов на данное устройство.

Процесс экспорта журналов событий "Аккорд-АМДЗ" в ПХЖ тогда будет выглядеть следующим образом. В некоторый момент времени пользователь подключает ПХЖ к компьютеру и при перезагрузке/старте ПЭВМ после процедур идентификации/аутентификации пользователя в "Аккорд-АМДЗ" и после взаимной аутентификации "Аккорд-АМДЗ" и ПХЖ до загрузки ОС журналы переносятся в память ПХЖ. ПХЖ должен быть зарегистрирован в АМДЗ по некоторому уникальному идентификатору, а используемый АМДЗ должен быть зарегистрирован в ПХЖ. Регистрация ПХЖ должна осуществляться через меню администрирования АМДЗ администратором информационной безопасности. После успешного экспорта в зависимости от выбранного режима (политики) журнал в "Аккорд-АМДЗ" может быть очищен.

Процесс переноса журналов из памяти ПХЖ в УСЖ может выглядеть аналогичным образом, с той лишь разницей, что производится не запись данных в ПХЖ, а их чтение. Журнал ПХЖ затем может быть очищен по специальной команде администратора после успешной аутентификации и авторизации или автоматически (по истечении установленного срока хранения или после каждого

удачного экспорта журналов). УСЖ извлекает журналы из ПХЖ, затем отправляет их в ЦХЖ, выполняя все операции в автоматическом режиме и не требуя от пользователей никаких действий.

Итак, схема работы построенного таким образом средства передачи журналов выглядит следующим образом.

- Первоначально производится настройка соответствующих экземпляров АМДЗ и ПХЖ для взаимной аутентификации (регистрация устройств в базах друг друга). Аналогичная настройка необходима и для взаимной аутентификации ПХЖ и УСЖ. Данные действия выполняются администратором информационной безопасности.

- Пользователь получает экземпляр ПХЖ, подключает его к АМДЗ и регулярно осуществляет перенос журналов в ЦХЖ с помощью УСЖ.

- При каждом подключении ПХЖ к УСЖ последнее производит все необходимые операции. Конкретная реализация УСЖ, канала связи между УСЖ и ЦХЖ и самого ЦХЖ зависит от конкретной ИС. Однако взаимодействие между УСЖ и ПХЖ в любом случае осуществляется с помощью специальной библиотеки для работы с ПХЖ.

Итак, приведен способ реализации безопасной промежуточной среды передачи журналов СДЗ и описано взаимодействие с данной средой СДЗ и УСЖ.

Подведем итоги.

- Центральное хранилище журналов можно физически отделить от компонентов ИС, что повышает уровень безопасности системы.

- СДЗ не взаимодействует с сетью, не нужно анализировать его уязвимости, связанные с сетевым взаимодействием, что позволяет упростить процедуру сертификации изделия СДЗ.

- Авторы добились того, что нужно обеспечивать лишь безопасную передачу данных с одного УСЖ на ЦХЖ, что гораздо проще, чем обеспечить безопасную передачу с множества СДЗ на ЦХЖ, так как не требует вмешательства разработчиков СДЗ.

- Конкретная реализация УСЖ, ЦХЖ и реализация канала передачи между ними зависят от модели угроз и бизнес-задач конкретной организации. Важно лишь, чтобы использовался интерфейс взаимодействия с ПХЖ, определённый его производителем. Разработчику СДЗ достаточно сосредоточиться на разработке системы журналирования (состоит из соответствующей подсистемы СДЗ, ПХЖ и библиотеки для работы с ним), которая является универсальной в том смысле, что может использоваться в разных ИС без привязки к конкретной инфраструктуре (аппаратной и про-

граммной составляющей, протоколам и используемым технологиям).

Следует отметить, что для корректной реализации описанной системы необходимо принять некоторые организационные меры, чтобы пользователи вовремя осуществляли перенос журналов и не допускали утери ПХЖ.

Литература

1. *Гарбузов Г.* Проведение расследований инцидентов ИБ: организационные и правовые аспекты [Электронный ресурс]. URL: <http://www.itsec.ru/articles2/control/provedeni-rassledovaniy-incidentov-ib> (дата обращения: 01.04.2017).

2. Работа с инцидентами информационной безопасности [Электронный ресурс]. URL: <https://habrahabr.ru/post/154405/> (дата обращения: 01.04.2017).

3. Стандарт Банка России СТО БР ИББС-1.0-2014 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения" [Электронный ресурс]. URL: https://www.cbr.ru/credit/Gubzi_docs/st-10-14.pdf (дата обращения: 24.03.2017)

4. Приказ ФСТЭК России от 11.02.2013 № 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" [Электронный ресурс]. URL: <http://fstec.ru/component/attachments/download/567> (дата обращения: 24.03.2017).

5. Приказ ФСТЭК России от 18.02.2013 № 21 "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" [Электронный ресурс]. URL: <http://fstec.ru/component/attachments/download/561> (дата обращения: 24.03.2017).

6. Приказ ФСТЭК от 14.03.2014 "Об утверждении Требований к обеспечению защиты информации в автоматизиро-

ванных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды" [Электронный ресурс]. URL: <http://fstec.ru/component/attachments/download/714> (дата обращения: 01.04.2017).

7. Методический документ ФСТЭК России "Профиль защиты средства доверенной загрузки уровня платы расширения четвертого класса защиты" [Электронный ресурс]. URL: <http://fstec.ru/component/attachments/download/661> (дата обращения: 24.03.2017).

8. Способ защиты от несанкционированного доступа к информации, хранимой на персональной ЭВМ. Патент на изобретение № 2475823. 20.02.2013. Бюл. № 5.

9. Методический документ ФСТЭК России "Меры защиты информации в государственных информационных системах" [Электронный ресурс]. URL: <http://fstec.ru/component/attachments/download/675> (дата обращения: 24.03.2017).

10. *Счастливый Д. Ю.* М&М!-платформа для защищенных мобильных систем // Вопросы защиты информации. 2016. № 2, С. 40—41.

11. *Алтухов А. А.* Контроль доступа на основе атрибутов и оптимизация управления множеством АПМДЗ: мат. XX Научно-практической конф. "Комплексная защита информации". Минск, 19—21 мая 2015 г. Минск: РИВШ, 2015. С. 55—60.

12. Руководство администратора (контроллеры Аккорд-5.5, Аккорд-5.5е, Аккорд-5.5МХ) [Электронный ресурс]. URL: http://www.accord.ru/docs/amdz/AMDZ_DOS_Admin_guide.pdf (дата обращения: 01.04.2017).

13. ГОСТ Р ИСО/МЭК 27002-2012 [Электронный ресурс]. URL: <http://docs.cntd.ru/document/1200103619> (дата обращения: 01.04.2017)

14. *Андреев В. М., Давыдов А. Н.* Безопасное хранение журналов работы СЗИ: мат. XX Научно-практической конф. Минск, 19—21 мая 2015 г. Минск: РИВШ, 2015. С. 49—52.

15. Специальный съемный носитель информации. Патент на полезную модель № 94751. 27.05.2010. Бюл. № 15.

Special removable device as a medium for transferring logs of trusted boot device

¹ *D. A. Epictetov;* ^{1,2,3} *A. A. Altukhov*

¹ Moscow institute of physics and technology (state university), Dolgoprudny, Moscow region, Russia

² Closed Joint Stock Company «ОКБ SAPR», Moscow, Russia,

³ National Research Nuclear University "MEPhI", Moscow, Russia

The article discusses the trusted boot device log collection method, based on the use of special information storage device and specially organized architecture of interaction of TBD and logs transfer and processing environment. The proposed method allows organizing a semi-automatic logs collection, eliminating the necessity to integrate the TBD into special logs collecting systems or to impose additional requirements to the information system that provides the transfer and collection of logs.

Keywords: logs collection, events registration, trusted boot device, log management, USB device with controlled access.

Bibliography — 15 references.

Received June 5, 2017