УДК 004.056.2

Предложения по архитектуре средства контроля конфигурации произвольных информационных систем

Н. В. Мозолина
Московский физико-технический институт (государственный университет),
г. Долгопрудный, Московская обл., Россия

Сформированы требования к системе контроля конфигурации (СКК) произвольной информационной системы. На основе полученных требований предложена архитектура СКК, в которой выделены универсальные (постоянные) и специализированные (переменные) структурные компоненты.

Ключевые слова: контроль целостности, конфигурация информационной системы.

Одним из необходимых объектов защиты информации является информационная технология (ИТ) — последовательность приемов, способов и методов применения средств вычислительной техники при выполнении функций сбора, хранения, обработки, передачи и использования данных. Обеспечение защищённости ИТ неразрывно связано с обеспечением защищенности той информационной системы (ИС), среды, в которой она реализуется [1, 2].

Конфигурации ИС, используемого в ней программного обеспечения (ПО) влияют на процессы реализации информационных технологий. Одна и та же программа при различных настройках может работать по-разному — реализовывать разные ИТ. В этом и заключается смысл изменения настроек. Некоторые конфигурации могут создавать угрозы безопасности, способствовать работе в системе "опасных" информационных технологий, поэтому очевидно, что необходимо контролировать не только отдельные элементы информационной системы, но и саму её конфигурацию [3].

Вопрос контроля конфигурации информационной системы можно рассматривать с нескольких точек зрения: во-первых, кто может влиять на её изменение (задача контроля доступа к настройкам ИС, например для виртуальных инфраструктур [4—6]); во-вторых, какие изменения являются допустимыми и разрешенными, а какие должны блокироваться (задача контроля целостности конфигурации ИС [3, 7]).

Решения этих задач не являются взаимозаменяемыми. С одной стороны, даже при обеспечении доступа только доверенных пользователей к разрешённым им функциям изменения конфигурации ИС необходимо проверять допустимость производимых ими настроек. С другой стороны, гарантируя пребывание системы только в некоторых разрешённых состояниях, т. е. контролируя целостность конфигурации, необходимо быть уверенным в том, что переход между этими состояниями осуществляется не случайным пользователем в случайный момент времени, а лишь при необходимости таких изменений.

Данная работа посвящена решению задачи контроля целостности конфигурации ИС. Разработаны требования к системе (система контроля конфигурации, СКК), решающей данную задачу. На основе этих требований предложены состав и структура системы, выделены постоянные и переменные структурные элементы.

Разработка требований к системе контроля конфигурации

Первым и основным требованием к СКК является возможность с её помощью задавать эталон конфигурации ИС (множество разрешённых состояний), считывать текущую конфигурацию и сравнивать её с эталонной, т. е. решать задачу контроля целостности конфигурации. В [3] описано применение атрибутной модели доступа для решения этой задачи. Будем опираться на полученный результат.

Все приведённые рассуждения не учитывали, с какой именно системой ведется работа: рассматривалась произвольная ИС. Это может быть, например, система виртуализации, построенная как на базе Microsoft Hyper-V, так и на основе VMware vSphere или QEMU/KVM, или распределённый вычислительный кластер, работающий на основе программной платформы Hadoop. Поэтому решение задачи контроля целостности конфигурации

Мозолина Надежда Викторовна, аспирант.
E-mail: nmozolina@okbsapr.ru

Статья поступила в редакцию 11 мая 2018 г.

должно быть универсальным и не зависеть от конкретной защищаемой системы.

Другим аргументом в пользу универсальности решения является тот факт, что представить себе однородную информационную систему сложно. ИС состоит из нескольких подсистем различного типа: распределённая подсистема хранения данных, подсистема терминального доступа и т. д. Естественно желание владельца ИС обладать единым инструментом для решения задачи контроля конфигурации всей системы, а не множеством различных средств для каждой из её подсистем.

В то же время системы различного типа имеют свои особенности. Они как минимум состоят из различных элементов. Кроме того, различаются связи (отношения) между этими элементами, различаются способы, с помощью которых возможно получить информацию о конфигурации системы. Таким образом, система контроля конфигурации должна учитывать уникальные особенности ИС различных типов, узко специализироваться на них.

Возникает противоречие. С одной стороны, СКК должна быть универсальной, с другой — специализированной, с одной стороны, работать вне зависимости от структуры и состава ИС, с другой — учитывать особые характеристики каждой подсистемы.

Данное противоречие легко устранить. Система контроля конфигурации должна обладать модульной архитектурой: лишь некоторые из её структурных элементов, которые непосредственно взаимодействуют с защищаемой ИС, должны зависеть от её типа и особенностей, ядро же СКК должно быть универсальным.

Также важным требованием является масштабируемость системы контроля конфигурации и возможность её адаптации к новым ИС. Это требование связано с непрерывным развитием информационных систем как количественным (ИС становятся больше, повышается число элементов в их составе), так и качественным (в ИС появляются подсистемы новых типов).

Кроме того, естественным требованием к СКК являются разделение его пользователей на привилегированных администраторов продукта и обычных пользователей системы контроля конфигурации, их идентификация и аутентификация. При этом необходимо отметить, что СКК предназначен для администраторов безопасности информационных систем, целостность конфигурации которых контролируется, и именно они будут "обычными пользователями СКК", выполняющими функции по созданию эталонов конфигурации систем, их применению, формированию запросов на проверку соответствия ИС заданному эталону и т. п. Задачей привилегированных администраторов СКК будет обеспечение работоспособности самой системы контроля конфигурации: её установка, настройка, регистрация обычных пользователей.

Помимо приведённых требований в СКК должен вестись журнал событий, что наряду с идентификацией и аутентификацией пользователей является традиционным требованием к средствам защиты информации.

Получен следующий список требований к системе контроля конфигурации:

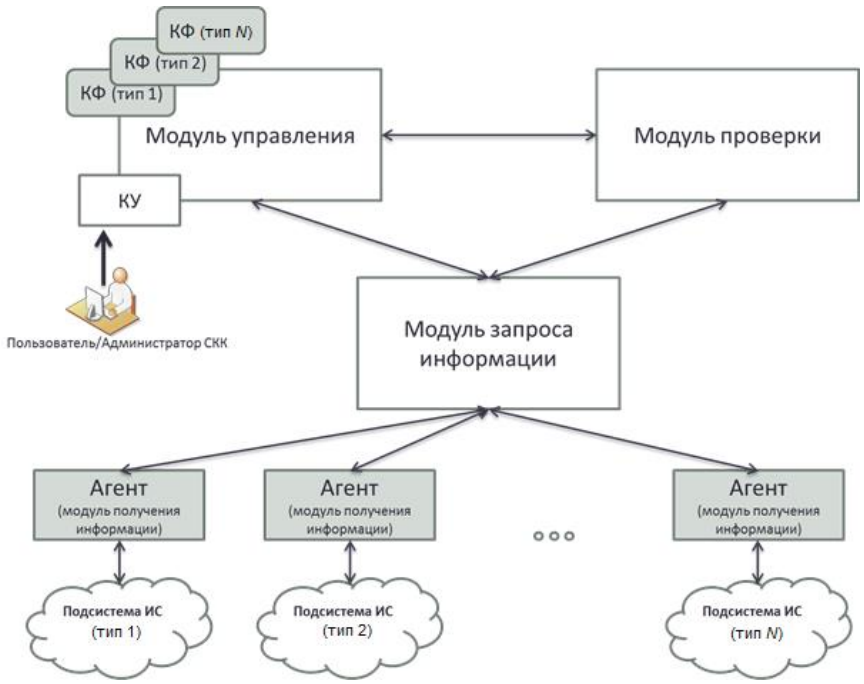
- возможность задания эталона (множества разрешённых состояний) ИС, его изменения и удаления;
- возможность считывания текущей конфигурации ИС;
- возможность сравнения текущей конфигурации ИС с эталоном;
- модульная архитектура, состоящая из универсального для любой ИС ядра СКК и специализированных модулей взаимодействия с различными типами информационных систем;
- масштабируемость и возможность адаптации к различным типам ИС;
- разделение пользователей СКК на обычных и привилегированных, их идентификация и аутентификация в системе;
- ведение журнала событий.

Предложения по архитектуре СКК

На основе разработанных требований предложены состав и структура системы контроля конфигурации (см. рис.). Приведём описание модулей СКК и их функциональных требований.

Модуль управления устанавливается на рабочее место администратора безопасности ИС (пользователя или администратора СКК). Этот структурный компонент отвечает за следующие функции:

- идентификация и аутентификация пользователей и администраторов СКК;
- формирование запроса (автоматически или по требованию пользователя) на получение данных о текущем состоянии ИС и передача его на модуль запроса информации;
- формирование запроса (автоматически или по требованию пользователя) на сравнение текущего состояния ИС и заданного эталона;
- работа с конфигурационными файлами (КФ): их импорт и удаление;
- предоставление пользователю возможности создать через консоль управления (КУ) эталон



Состав и структура системы контроля конфигурации

конфигурации ИС (её подсистемы указанного типа) на основе конфигурационного файла и данных о текущем её состоянии;

- предоставление пользователю возможности изменения и удаления эталона;
- ведение архива применяемых эталонов;
- передача данных об установленных эталонах и изменениях в них модулю проверки;
- отображение в КУ текущего состояния системы;
- сбор событий СКК, хранение журнала событий, отображение его для пользователя в КУ;
- работа с несколькими модулями проверки.

Конфигурационный файл представляет собой обобщённое описание ИС определённого типа: наборы элементов в неё, возможные связи между ними. КФ уникален для каждого типа ИС.

Эталон задаётся для каждой подсистемы ИС, так как зависит от её структурных особенностей. Вместе с тем эталоны имеют единый формат, позволяющий модулю проверки работать с ними вне зависимости от того, к системам каких типов эти эталоны относятся. Эталоном ИС является совокупность эталонов её подсистем.

Созданные пользователем в КУ эталоны передаются на модуль проверки, где заменяют старые эталоны. На модуле управления старые эталоны сохраняются в архиве. Срок хранения эталонов определяется администратором СКК через КУ. Старые эталоны могут быть возвращены пользователем из архива и применены.

Модуль проверки может быть установлен как на рабочем месте администратора безопасности (там же, где и модуль управления), так и на отдельный сервер. Этот структурный компонент отвечает за следующие функции:

- получение эталонов от модуля управления;
- формирование запроса на получение информации о текущем состоянии ИС к модулю запроса информации и получение соответствующих данных;
- сравнение текущего состояния ИС с эталоном (при получении соответствующего запроса от модуля управления) – проверка конфигурации;
- формирование результата проверки конфигурации и передача его на модуль управления;
- работа с несколькими модулями управления.

Результатом сравнения эталона ИС и её текущей конфигурации должна быть информация о нарушении или сохранении целостности конфигурации. В случае нарушения должна получаться информация о некорректных настройках (атрибутах системы).

Модуль запроса информации может быть установлен как на рабочем месте администратора безопасности (там же, где и модуль управления), так и на отдельный сервер. Этот структурный компонент отвечает за следующие функции:

- получение информации об ИС от агентов (модулей получения информации) по запросу модуля управления или модуля проверки;

- передача полученных от агентов данных модулям проверки и управления;
- работа с несколькими модулями управления, проверки и несколькими агентами.

Агент (*модуль получения информации о системе*) отвечает за следующие функции:

- получение данных из подсистемы ИС по запросу модуля запроса информации;
- преобразование полученных данных в стандартный вид, универсальный для всех систем и удобный для получения модулем запроса информации;
- передача данных модулю запроса информации.

Зависимость выделенных модулей от контролируемой ИС: непосредственно с защищаемой ИС (её подсистемами) происходит взаимодействие лишь агентов (модулей получения информации), поэтому лишь этот структурный элемент должен быть специализированным, своим для каждой подсистемы ИС; все другие модули СКК являются универсальными (постоянными) и не зависят от защищаемой системы. Возможность работы пользователей СКК с системами различных типов и построение эталонов модулей управления для них обеспечивается за счёт конфигурационных файлов, загружаемых в модуль управления. На рисунке переменные структурные компоненты СКК, зависящие от типа контролируемой системы, выделены серым цветом.

Заключение

Сформулированы требования к системе контроля конфигурации произвольной информационной системы. На основе полученных требований предложена архитектура СКК, в которой выделены универсальные (постоянные) и специализированные (переменные) структурные компоненты.

Литература

1. *Конявский В. А.* Научно-методические проблемы создания защищенных информационных технологий // ВКСС Connect! 2006. № 1 (34). С. 41—43.
2. *Конявская С. В.* К вопросу о классификации объектов защиты информации // Безопасность информационных технологий. 2013. № 3. С. 14—18.
3. *Мозолина Н. В.* Решение задачи контроля целостности конфигурации, основанное на атрибутной модели контроля доступа // Вопросы защиты информации. 2017. № 3. С. 23—25.
4. *Конявская С. В., Угаров Д. В., Постоев Д. А.* Инструмент контроля доступа к средствам управления виртуальной инфраструктурой // Информационная безопасность. 2016. № 2. С. 9.
5. *Угаров Д. В., Постоев Д. А*. Проблемы реализации разграничения доступа к функциям управления виртуальных сред // Вопросы защиты информации. 2016. № 3. С. 34—35.
6. *Журов П. М.* Разграничение доступа к функциям управления средства виртуализации VMware vSphere: тр. 60-й Всеросс. науч. конф. МФТИ. 26—27 ноября 2017 г. Москва, Долгопрудный, Жуковский, 2017. С. 184—185.
7. *Мозолина Н. В.* Контроль целостности виртуальной инфраструктуры и ее конфигурации // Вопросы защиты информации. 2016. № 3. С. 31—33.

Architecture proposals of configuration control system for arbitrary information systems

N. V. Mozolina
Moscow Institute of Physics and Technology (State University),
Dolgoprudny, Moscow region, Russia

In the article requirements to the configuration control system (CCS) of an arbitrary information system were formed. Based on the received requirements the CCS architecture was proposed. Universal (permanent) and specialized (variable) structural components were distinguished in the CCS.

Keywords: integrity control, information system configuration.

Bibliography — 7 references. *Received May 11, 2018*