УДК 004.056.2

**КОНТРОЛЬ КОНФИГУРАЦИИ
ПРОИЗВОЛЬНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ.
ПРЕДЛОЖЕНИЯ ПО АРХИТЕКТУРЕ РЕШЕНИЯ**

Н.В. МОЗОЛИНА

*МФТИ (ГУ), Москва, 117303, Россия*

**Введение**

Одним из 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». Необходимость защищать ИТ осознана недавно, и на сегодня предложен лишь один подход к её защите – использование кодов аутентификации. В этом случае контроль осуществляется в динамике, во время исполнения информационной технологии, – происходит проверка, что последовательность действий, составляющих эту ИТ, не нарушена. В случае обнаружения нарушений исполнение прекращается [1–3].

Помимо динамического контроля ИТ имеет смысл рассматривать и статическую сторону вопроса – какие ИТ в принципе могут быть реализованы в нашей информационной системе (ИС) и на исполнение какой она настроена в данный момент. На это влияют конфигурации ИС, используемого в ней программного обеспечения (ПО): одна и та же программа при различных настройках, может работать по-разному – реализовывать разные ИТ, собственно, в этом и заключается смысл изменения этих настроек. Некоторые же конфигурации могут создавать и реализовывать угрозы безопасности, способствовать работе в системе незащищённых и вредоносных информационных технологий. Становится понятным, что для статического контроля ИТ необходимо контролировать конфигурацию ИС [4].

 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 [5–7]), во-вторых, какие изменения являются допустимыми и разрешёнными, а какие должны блокироваться (задача контроля целостности конфигурации ИС [4, 8]).

Стоит заменить, что решение одной из этих задач не является альтернативой решению другой. Так даже при обеспечении доступа только доверенных пользователей только к разрешённым им функциям изменения конфигурации ИС, необходимо проверять, что производимые настройки допустимы. С другой стороны, если мы гарантируем пребывание системы только в некоторых разрешённых состояниях, то есть контролируем целостность конфигурации, необходимо быть уверенным, что переход между этими состояниями осуществляется не случайным пользователем в случайный момент времени, но лишь при необходимости таких изменений.

И всё же данная работа посвящена лишь решению задачи контроля целостности конфигурации ИС. В статье предлагаются требования к системе, решающей данную задачу (будем называть её системой контроля конфигурации, СКК), а также разработанные на их основе состав и структура системы с выделенными в ней постоянными и переменными структурными элементами.

**Разработка требований к системе контроля конфигурации**

Первым и основным требованием к СКК является возможность с её помощью задавать эталон конфигурации ИС (множество разрешённых состояний [4]), считывать текущую конфигурацию и сравнивать её с эталонной, то есть решать задачу контроля целостности конфигурации. В [4] описано применение атрибутной модели доступа для решения этой задачи. В данной работе будем опираться на полученный результат.

Другим требованием к СКК является его универсальность.

В наше время сложно представить себе однородную информационную систему. Современная ИС состоит как бы из нескольких подсистем различного типа: распределённая подсистема хранения данных, подсистема терминального доступа и так далее. Вообще, делить ИС на подсистемы можно различными способами, например, по типу информации, которая обрабатывается, по географическому расположению, по функциональному предназначению. В данной статье подсистема, её тип будут определяться тем программным обеспечением, которое её формирует. Так в случае одновременного использования в ИС виртуализации, построенной на базе различных платформ, будут выделены соответственно подсистемы различного типа, например, подсистема на основе VMware vSphere и подсистема на основе Microsoft Hyper-V. Такое деление связано с различием тех объектов, которые входят в состав подсистемы, а также с различием в способе получения информации о конфигурации выделенной подсистемы.

Естественно желание владельца ИС «не плодить сущности», то есть обладать единым инструментом для решения задачи контроля конфигурации всей системы, а не множеством различных средств для каждой из её подсистем.

Примечательно также, что во всех приведённых выше рассуждениях не учитывалось, конфигурация какой именно ИС рассматривается. Это могла быть, например, и система виртуализации, построенная как на базе Microsoft Hyper-V, так и на основе VMware vSphere или QEMU/KVM, и распределённый вычислительный кластер, работающий на основе программной платформы Hadoop. Это говорит о том, что задача контроля целостности конфигурации актуальна для произвольной системы, и потому следует искать универсальное решение, не зависящее от конкретной защищаемой системы.

В то же время подсистемы различного типа из состава ИС 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. То есть система контроля конфигурации должна учитывать уникальные особенности подсистем различных типов, узко специализироваться на них.

Это приводит нас, казалось бы, к противоречию. 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.

На самом деле противоречие легко устраняется. 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, развитием 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 будет разделение его пользователей на привилегированных администраторов продукта и на обычных пользователей системы контроля конфигурации, их идентификация и аутентификация. При этом название вторых, «обычные пользователи» не должно никого обманывать – 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 же привилегированных администраторов СКК будет являться обеспечение работоспособности самой системы контроля конфигурации – её установка, настройка, регистрация обычных пользователей, наделение их разными наборами прав.

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

Так получен следующий список требований к системе контроля конфигурации:

1. возможность задания эталона (множества разрешённых состояний) ИС, в том числе, его изменение и удаление;
2. возможность получения информации о текущей конфигурации ИС;
3. возможность сравнения текущей конфигурации ИС с эталоном, определения тех настроек конфигурации, которые привели к нарушению целостности, информирование администраторов безопасности о произошедшем инциденте;
4. модульная архитектура, состоящая из универсального для любой ИС ядра СКК и специализированных модулей взаимодействия с различными типами подсистем;
5. масштабируемость и возможность адаптации к подсистемам новых типов;
6. разделение пользователей СКК на обычных и привилегированных, их идентификация и аутентификация в системе;
7. ведение журнала событий.

**Предложения по архитектуре СКК**

На основе разработанных в предыдущем разделе требований предлагаются состав и структура системы контроля конфигурации (рисунок 1). Приведём описание модулей СКК и функциональных требований к ним.

*Модуль управления* предназначен для работы администратора безопасности ИС (пользователя или администратора СКК). Этот структурный компонент отвечает за следующие функции:

1. идентификация и аутентификация пользователей и администраторов СКК;
2. формирование запроса (автоматически или по требованию пользователя) на получение данных о текущем состоянии ИС и передача его на модель запроса информации;
3. формирование запроса (автоматически или по требованию пользователя) на сравнение текущего состояния ИС и заданного эталона;
4. работа с конфигурационными файлами (КФ): их импорт и удаление;
5. предоставление пользователю возможности создать через консоль управления (КУ) эталон конфигурации ИС (её подсистемы указанного типа) на основе конфигурационного файла и данных о текущем её состоянии;
6. предоставление пользователю возможность изменения и удаления эталона;
7. ведение архива применяемых эталонов;
8. передача данных об установленных эталонах и изменениях в них модулю проверки;
9. отображение в КУ текущее состояние системы;
10. сбор событий СКК, хранить журнал событий, отображать его для пользователя в КУ;
11. работа с несколькими модулями проверки.

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

Эталон задаётся свой 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 относится. Эталоном ИС является совокупность эталонов её подсистем.

*Рисунок 1 Состав и структура системы контроля конфигурации*

Созданные пользователем в КУ эталоны передаются в модуль проверки, где заменяют старые эталоны. В модуле управления старые эталоны сохраняются в архив, срок хранения эталонов определяется администратором СКК через КУ. Старые политики 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 отдельном сервере. Этот структурный компонент отвечает за следующие функции:

1. получение эталонов от модуля управления;
2. формирование запроса на получение информации о текущем состоянии ИС к модулю запроса информации и получение соответствующих данных;
3. сравнение текущего состояния ИС с эталоном (при получении соответствующего запроса от модуля управления) – проверка конфигурации;
4. формирование результата проверки конфигурации и передача его на модуль управления;
5. 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 должны быть определены те настройки (значения атрибутов системы), повлекшие за собой обнаруженное нарушение. Информация должна быть передана на модуль управления для информирования администратора безопасности (пользователя СКК) о возникшем инциденте.

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

1. получение информации об ИС от агентов (модулей получения информации) по запросу модуля управления или модуля проверки;
2. передача полученных от агентов данных модулям проверки и управления;
3. работа с несколькими модулями управления, проверки и несколькими агентами.

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

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

Помимо описания функциональных требований к модулям СКК, стоит решить вопрос зависимости выделенных модулей от контролируемой ИС. Непосредственно с защищаемой ИС (её подсистемами) взаимодействуют только агенты (модули получения информации), а потому 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. Переменные структурные компоненты СКК, зависящие от типа контролируемой системы, на рисунке 1 выделены серым цветом.

**Заключение**

Представленные в статье архитектура и состав СКК показывают потенциальную возможность спроектировать средство, решающее задачу контроля конфигурации ИС.

Обоснование реализуемости предложенного проекта, разработка протоколов взаимодействия между модулями СКК, формат конфигурационных файлов – предмет дальнейших исследований и будут освещены в будущих статьях.

**Список литературы**

1. *Конявский В. А.*Информационные технологии как объект защиты и классификация антивирусных программ // Безопасность сетей и средств связи. Вып. 2. 2007. С. 52–54.
2. *Конявский В. А.*  Научно-методические проблемы создания защищенных информационных технологий // ВКСС Connect! М., 2006. № 1 (34). С. 41–43.
3. *Конявская С. В.*  К вопросу о классификации объектов защиты информации // Безопасность информационных технологий. М., 2013. № 3. С. 14–18.
4. *Мозолина Н. В.* Решение задачи контроля целостности конфигурации, основанное на атрибутной модели контроля доступа. // Вопросы защиты информации, 2017. № 3. С. 23–25.
5. *Конявская С. В., Угаров Д. В., Постоев Д. А.* Инструмент контроля доступа к средствам управления виртуальной инфраструктурой // Information Security/Информационная безопасность. М., 2016. № 2. С. 9.
6. *Угаров Д. В., Постоев Д. А*. Проблемы реализации разграничения доступа к функциям управления виртуальных сред // Вопросы защиты информации: Научно-практический журнал/ФГУП «ВИМИ». М., 2016. Вып. 3. № 114. С. 34–35.
7. *Журов П. М.* Разграничение доступа к функциям управления средства виртуализации VMware vSphere // Труды 60-й Всероссийской научной конференции МФТИ (26–27 ноября 2017 года). М., Долгопрудный, Жуковский. 2017. С. 184–185.
8. *Мозолина Н. В.* Контроль целостности виртуальной инфраструктуры и ее конфигурации // Вопросы защиты информации: Научно-практический журнал/ФГУП «ВИМИ». М., 2016. Вып. 3. № 114. С. 31–33.