УДК 004.056

Реализация концепции управления конфигурациями при помощи программного модуля "Паспорт ПО"

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

Рассмотрены основные принципы концепции управления конфигурациями, ориентированного на безопасность. Продемонстрирована возможность реализации этих принципов при решении задачи контроля конфигурации рабочих мест пользователей при помощи программного модуля "Паспорт ПО".

Ключевые слова: управление конфигурациями, контроль конфигурации, администрирование.

Авторы различных научных статей [1, 2] и учебников [3—5] по защите информации, специалисты компаний, разрабатывающих системы безопасности [6], едины в вопросе построения систем защиты. Их создание начинают с анализа текущего состояния информационной системы (ИС), для которой разрабатывают защиту, с определения объектов защиты, а также с построения модели угроз. Завершающим этапом является сопровождение разработанной системы, т. е. ее непрерывный мониторинг, контроль состояния и конфигураций, причем этот контроль необходимо осуществлять в течение всей жизни ИС вплоть до ее ликвидации. Указанный подход к построению систем защиты нашел свое отражение и в национальном стандарте [7], а в концепции управления конфигурациями, ориентированного на безопасность (Security-Focused Configuration Management of Information Systems, SecCM) [8], приведены основные принципы, позволяющие организовать повышение защищенности информационной системы за счет управления ее конфигурациями.

Изучим методы контроля состояния рабочих мест пользователя, а также рассмотрим особенности этого контроля при помощи программного модуля (ПМ) "Паспорт ПО" [9] с точки зрения повышения защищенности системы.

Материалы и методы

Для большинства информационных систем характерны постоянные изменения в результате установки нового программного и аппаратного обеспечения, его обновления или удаления, создания документов, баз данных и т. д. Конфигурация системы и ее компонентов оказывает прямое влияние на состояние безопасности. Изменения, происходящие на рабочих местах пользователей, могут быть как результатом санкционированных действий (например, обновление версии программных модулей администратором), так и результатом работы некоторого вредоносного программного обеспечения (ПО), случайного или намеренного внесения нежелательных изменений пользователем.

Последствиями несанкционированных изменений могут быть нерациональное использование рабочего времени за счет использования служебных компьютеров в личных целях, угрозы безопасности и промышленный шпионаж из-за установки пользователями потенциально или заведомо опасных программ и даже полное нарушение работоспособности системы [9].

Для своевременного обнаружения и предотвращения таких изменений недостаточно организационных мер (инструкций, регламентов), необходим постоянный мониторинг состояния рабочих мест пользователя. Обеспечить такой контроль может программный модуль "Паспорт ПО" (ПМ "Паспорт ПО"), разработанный для анализа программной среды компьютеров под управлением ОС Windows.

Рассмотрим применение ПМ "Паспорт ПО" и покажем, как его функциональные возможности позволяют реализовать ключевые принципы управления конфигурациями, ориентированного на безопасность. Проанализируем данные, полученные из литературных источников, проведем аналогию между изученными возможностями.

Мозолина Надежда Викторовна, аспирант.
E-mail: mozolina@phystech.edu

Статья поступила в редакцию 22 сентября 2020 г.

Результаты изучения материалов и методов

Управление конфигурациями, ориентированное на безопасность, — одна из концепций повышения защищенности информационной системы за счет управления ее конфигурациями. Реализация принципов SecCM заключается в:

- идентификации и записи конфигураций, которые влияют на состояние безопасности системы и организации;
- учете рисков безопасности при утверждении начальной конфигурации;
- анализе последствий изменения конфигурации системы для безопасности;
- документировании одобренных и внедренных изменений [8].

Важность управления конфигурациями, ориентированного на безопасность, заключается в возможности с его помощью сократить время обнаружения компрометации компонента информационной системы, уменьшить влияние атаки за счет ее раннего обнаружения, снизить принесенный ущерб [10, 11].

В [8] указаны основные действия, выполнение которых позволяет реализовать корректное управление конфигурациями в информационной системе. Так, ключевыми этапами являются планирование SecCM (разработка политик применения средства SecCM), внедрение SecCM (определение базовых конфигураций и их утверждение), контроль изменений конфигурации (использование некоторой панели управления конфигурации для рассмотрения и утверждения изменений в ИС) и мониторинг уже утвержденных конфигураций.

ПМ "Паспорт ПО" предназначен для автоматизации контроля целостности состояния программной среды (основных характеристик файлов программного обеспечения) и контроля изменений состава ПО (установленные на средство вычислительной техники системные и прикладные программные продукты). Назовем конфигурацией СВТ программную среду вместе с совокупностью состава ПО. Фиксацию состояния конфигурации СВТ выполняют через создание записей специального вида — проектов паспортов ПО. Заверенный (подписанный электронной подписью) проект паспорта называют паспортом ПО. Он представляет эталонное состояние конфигурации СВТ. Для формирования паспорта ПО пользователь должен обладать в рамках ПМ "Паспорт ПО" правом на подпись проекта.

Основными элементами ПМ "Паспорт ПО" являются:

- серверный компонент (Сервер) с базой данных;
- компонент управления (АРМ управления);
- клиентский компонент (Клиент), устанавливаемый на подконтрольные объекты (ПКО), рабочие места (СВТ), конфигурацию которых контролирует программный модуль;
- сервис обмена сообщениями RabbitMQ, обеспечивающий взаимодействие по сети между всеми элементами [12].

Подготовка системы для работы ПМ "Паспорт ПО" заключена в выполнении следующих действий:

- регистрация учетных записей административного персонала, отвечающего за контроль целостности программной среды в АРМ управления, формирование ролей и назначение их учетным записям;
- формирование списка ПКО с разбиением на логические группы (подразделения);
- формирование общей базы шаблонов (прототипов конфигураций рабочих мест пользователей);
- назначение шаблонов подконтрольным объектам;
- проведение опроса на ПКО (сканирования конфигурации СВТ в соответствии с назначенным шаблоном) и формирование его паспорта ПО.

Покажем, что указанные действия могут быть рассмотрены как выполнение этапов планирования SecCM и внедрения SecCM.

В результате подготовки системы в базе данных ПМ "Паспорт ПО" формируются записи об эталонном состоянии конфигурации СВТ с установленным Клиентом. В ходе дальнейшей работы выполняют сканирование подконтрольных объектов по заданному для СВТ расписанию или по запросу управляющего персонала ПМ "Паспорт ПО". В ходе сканирования Клиент определяет конфигурацию СВТ и отправляет информацию на Сервер, который автоматически сверяет полученные данные о текущем состоянии ПКО с эталонным и информирует управляющий персонал ПМ "Паспорт ПО" о выявленных нарушениях. Для каждого ПКО в случае обнаружения нарушений должен быть выполнен анализ возникших изменений, в результате которого возможны обновление паспорта ПО в случае санкционированных модификаций или же принятие мер по устранению причин возникших несоответствий, разбор инцидента безопасности. Данные операции являются третьим этапом реализации SecCM.

Информацию обо всех действиях по формированию как проектов паспортов ПО, так и самих паспортов ПО сохраняют в журнале событий ПМ "Паспорт ПО". Анализ сообщений из журнала событий позволяет производить выявление изменений в уже утвержденных паспортах, реализуя тем самым этап мониторинга SecCM.

Рассмотрев основные функции ПМ "Паспорт ПО" и сопоставив этапы его применения с этапами реализации концепции SecCM, выполним сравнение основных процессов и объектов, на которые опирается стандарт SecCM [8, с. 17, 18], и процессов и объектов, которыми оперирует программный модуль. Результат такого сравнения представлен в таблице.

Обсуждение

Приведенное сопоставление, а также соответствие между этапами SecCM и этапами применения ПМ "Паспорт ПО" показывает, что программный модуль может быть рассмотрен как средство, реализующее управление конфигурациями, ориентированное на безопасность.

Стоит отметить, что рассмотренный ПМ "Паспорт ПО" является наложенным средством контроля изменений рабочих мест пользователя.

В то же время использование большого числа компьютеров под управлением ОС Windows почти всегда сопровождается их объединением с использованием службы каталогов Active Directory (AD) в единый домен.

Эта служба позволяет управлять различными объектами (рабочими компьютерами, серверами, принтерами, пользователями и т. д.) из единой точки (контролера домена), а также получать сведения о состоянии объектов и об их изменениях [13], т. е. выполнять мониторинг конфигураций.

Итак, мы сталкиваемся с необходимостью наложенного средства даже при условии, что в системе есть встроенная система с аналогичной функциональностью.

Результаты сравнения процессов

NIST.SP.800-128	ПМ "Паспорт ПО"
Управление конфигурацией (Configuration Management — CM) — набор действий, направленных на создание и поддержание целостности продуктов и систем посредством контроля процессов создания, изменения и мониторинга конфигураций этих продуктов и систем	Набор действий по формированию базы шаблонов (типовых конфигураций СВТ), назначению их рабочим местам пользователей, формированию паспортов ПО, проведению сканирования рабочих мест и сравнению текущей конфигурации СВТ (проекта паспорта) с эталонной (паспорт ПО)
Элемент конфигурации (Configuration Item — CI) — идентифицируемая часть системы (например, аппаратное обеспечение, программное обеспечение, встроенное ПО, документация или их комбинация), которая является дискретной целью процесса управления конфигурацией	Подконтрольный объект (ПКО) — СВТ с установленным на него Клиентом ПМ "Паспорт ПО" — однозначно идентифицируется именем ПКО. Обеспечение контроля целостности конфигурации ПКО является целью применения ПМ "Паспорт ПО"
Базовая конфигурация (Baseline Configuration) — набор спецификаций для системы или элемента конфигураций в системе, который был рассмотрен и согласован в определенный момент времени и который может быть изменен только через процедуры контроля изменений	Паспорт ПО — заверенный проект паспорта ПО, содержащий информацию о конфигурации СВТ. Процесс заверения проекта заключается в его подписи пользователем ПМ "Паспорт ПО". Формирование нового паспорта ПО для СВТ возможно лишь в результате формирования нового проекта паспорта ПО, его сопоставления с действующим паспортом, а также подписи данного проекта
План управления конфигурацией (Configuration Management Plan — CM Plan) — полное описание ролей, обязанностей, политики и процедуры, применяемых при управлении конфигурацией продуктов и системы	ПМ "Паспорт ПО" является инструментом контроля целостности состояния программной среды. Регламент его применения для мониторинга конфигураций рабочих мест пользователей информационной системы может быть рассмотрен как план управления конфигурацией

Хотя использование встроенных в AD технологий позволяет осуществлять контроль изменений рабочих мест, применение данной службы каталогов порождает "проблему суперпользователя", т. е. сосредоточения максимальных привилегий в рамках одной роли (в данном случае — в рамках роли администратора домена). Обладая полными правами, пользователь с указанной ролью может вносить любые изменения, что делает бессмысленным возложение на него обязанностей по контролю этих изменений и требует создания отдельных учетных записей с усеченной ролью для мониторинга. Создание для пользователей учетных записей, назначение учетным записям ролей может выполнять администратор домена. В то же время это нарушает концепцию разделения ролей администратора и администратора информационной безопасности (ИБ).

Аналогично использованию ПАК "Сегмент-В" для управления доступом в виртуальной инфраструктуре VMware vSphere [14] применение наложенного средства контроля изменений позволяет избежать "проблемы суперпользователя", а также смешения прав и обязанностей администратора и администратора ИБ.

Таким образом, наложенное средство контроля хотя частично и дублирует встроенную функциональность, но является необходимым компонентом защищенной информационной системы.

Заключение

При построении системы защиты некоторой ИС следует помнить, что данный процесс не завершается вводом средств защиты информации в эксплуатацию, их настройкой. Контроль состояния и конфигурации каждого элемента должен выполняться в течение всей жизни информационной системы. Для выполнения этого контроля необходим комплексный подход: как разработка различных регламентов по порядку внесения изменений, так и применение автоматизированных средств контроля конфигураций. Программный модуль "Паспорт ПО" позволяет решить задачу контроля изменений конфигурации рабочих мест пользователей, реализуя принципы управления конфигурациями, ориентированного на безопасность.

Литература

1. *Селищев В. А., Чечуга О. В., Наседкин М. Н.* Построение системы информационной безопасности предприятия // Изв. ТулГУ. Технические науки. 2009. № 1, 2 [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/postroenie-sistemy-informatsionnoy-bezopasnosti-predpriyatiya (дата обращения: 13.08.2020).
2. *Гудков С. Н., Коробкин Д. И., Рогозин Е. А.* Основные этапы и задачи проектирования программных систем защиты информации в автоматизированных системах // Вестник ВГТУ. 2009. № 10 [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/osnovnye-etapy-i-zadachi-proektirovaniya-programmnyh-sistem-zaschity-informatsii-v-avtomatizirovannyh-sistemah (дата обращения: 05.09.2020).
3. *Внуков А. А.* Защита информации в банковских системах: учебное пособие для бакалавриата и магистратуры. Изд. 2-е, испр. и доп. — М: Юрайт, 2018. — 246 с.
4. *Ясенев В. Н.* Конспект лекций по информационной безопасности [Электронный ресурс]. URL: http://www.iee.unn.ru/wp-content/uploads/sites/9/2017/02/konspekt-lektsij-po-IB.pdf С. 110-112 (дата обращения: 05.09.2020).
5. *Гришина Н. В.* Организация комплексной системы защиты информации. — М.: Гелиос АРВ, 2007. — 256 с.
6. Создание системы защиты персональных данных, приведение процессов обработки и обеспечения безопасности персональных данных в соответствие требованиям законодательства [Электронный ресурс]. URL: https://www.dialognauka.ru/services/creation_system_security_personal_data/ (дата обращения: 13.09.2020).
7. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.
8. Guide for Security-Focused Configuration Management of Information Systems [Электронный ресурс]. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf (дата обращения: 13.09.2020).
9. Сайт компании ОКБ САПР. Паспорт ПО [Электронный ресурс]. URL: https://www.okbsapr.ru/products/management/software-passport/ (дата обращения: 05.09.2020).
10. *Jackson B.* Why Security Configuration Management (SCM) Matters [Электронный ресурс]. URL: https://www.tripwire.com/state-of-security/security-data-protection/security-configuration-management/why-security-configuration-management-matters/ (дата обращения: 13.09.2020).
11. *Crast F.* NIST issues Security-Focused Configuration Management Guidelines [Электронный ресурс]. URL: https://www.securezoo.com/2019/11/nist-issues-security-focused-configuration-management-guidelines/ (дата обращения: 13.09.2020).
12. Программный модуль автоматизированного форматирования паспортов программного обеспечения автоматизированных рабочих мест и серверов "Паспорт ПО". Общее описание 11443195.501410.080 94 [Электронный ресурс]. URL: https://www.okbsapr.ru/upload/iblock/ecb/ecbafca5423510fd018bc3e32c6b8c9a.pdf
13. Active Directory Domain Services Overview [Электронный ресурс]. URL: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview (дата обращения: 13.09.2020).
14. *Угаров Д. В., Постоев Д. А.* Проблемы реализации разграничения доступа к функциям управления виртуальных сред // Вопросы защиты информации. 2016. Вып. 3. № 114. С. 34, 35.

Implementation of the configuration management concept using the software module "Passport PO"

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

The article discusses the basic principles of the concept of Security-Focused Configuration Management of Information Systems as well as the possibility of their implementation to control the configuration of working met users using the software module "Passport PO".

Keywords: configuration management, configuration control, administration.

Bibliography — 14 references. *Received September 22, 2020*