Формирование профилей стандартов в обеспечение требуемого уровня качества информационной безопасности

Мухамедзянов Геннадий Ильгизарович
Аспирант
Национальный исследовательский университет Высшая школа экономики, Rambler Group
123458, Москва, Таллинская ул. 34
g.mukhamedzyanov@rambler-co.ru

Старых Владимир Александрович
к.т.н., доцент, профессор
Национальный исследовательский университет Высшая школа экономики
123458, Москва, Таллинская ул. 34
vstarykh@hse.ru

Аннотация: Цель данной статьи - формирование теоретических основ, анализ рабочих инструментов и технологий для построения информационной системы, позволяющей оптимизировать сканирование ИС на соответствие стандартам информационной безопасности, анализ полученных данных и определение взаимосвязей различных требований соответствующих стандартов. Такая информационная система позволит провести оптимизацию бизнес-процессов по управлению ИБ, сократить количество ошибок конфигурирования, уменьшить влияние человеческого фактора при построении комплексов ИС. В статье приведено исследование на тему использования профилей стандартов при проверке соответствия предприятия внешним и внутренним стандартам ИБ, таких как СТО БР ИББС, PCI DSS, ISO2700x и т.д. Рассмотрены существующие технологические средства автоматизации проверок соответствия стандартов такие как SCAP, XCCDF.

Ключевые слова: информационная безопасность, **с**тандарт ИБ, соответствие стандартам, PCI DSS, СТО БР ИББС, SCAP, CIS, NIST.

Forming profile of standards to ensure the required level quality of information security

Vladimir A. Starykh
Prof. of School of Computer Engineering
National Research University Higher School of Economics
Moscow, Russia, 123458
vstarykh@hse.ru

Gennadiy I. Mukhamedzyanov
PhD student, Postgraduate School of Technical Sciences
National Research University Higher School of Economics
Moscow, Russia, 123458
g.mukhamedzyanov@rambler-co.ru

Abstract: The purpose of this article - the forming of theoretical foundations, analysis of working tools and technologies for the construction of an information system that allows to optimize the scanning of IS for compliance with information security standards, the analysis of the data and the definition of the relationship of the various requirements of the relevant standards. Such information system will allow to optimize business processes for is management, to reduce the number of configuration errors, to reduce the influence of the human factor in the construction of is complexes. The article presents a study on the use of standards profiles when checking the company's compliance with external and internal standards of information security.

Keywords: information security, quality, standard, compliance, PCI DSS, SCAP, CIS, NIST.

1 Введение

В Доктрине безопасности Российской Федерации [1] чётко сформулирована конкретная задача ликвидации зависимости отечественной промышленности от зарубежных информационных технологий и средств обеспечения ИБ (ст.25). Одной из основных задач отделов информационной безопасности в компаниях является обеспечение требуемого уровня качества информационной безопасности ИС, в части обеспечения снижения количества уязвимостей, увеличения надежности защищаемых ИС, приведения доступности к требуемому уровню.

Одним из методов повышения уровня информационной безопасности предприятия является приведение информационных систем к определенным стандартам и нормам безопасного конфигурирования.

При сканировании операционных систем сканерами уязвимостей с функцией проверки на соответствие стандартам информационной безопасности, - приходится многократно нагружать сетевое оборудование, рабочие станции и серверы техническими проверками, связанными с конкретными требованиями определенных стандартов. Когда появляется необходимость проверить соответствие другому стандарту, сканирование повторяется с другим профилем, который соответствуют другому стандарту. Рутинное по характеру, сравнение полученных результатов ложится на плечи системных администраторов или специалистов по безопасности.

Целью данной статьи является формулировка задачи возможности объединения различных стандартов в единый профиль, что позволит значительно уменьшить время сканирования ИС на соответствие стандартам ИБ за счет единовременных проверок идентичных требований стандартов. К тому же может потребоваться не множественные сканирования одних и тех же параметров ИС, а единственное сканирование, что позволит снизить общую нагрузку на соответствующие компоненты проверяемых ИС.

Современным компаниям приходится на стратегическом уровне определяться с политиками и стандартами информационной безопасности, то есть переносить их в практическую плоскость в область стратегического управления. Но для этого необходимо применять на практике общепринятые международные, гармонизированные и локальные стандарты и практики по ИБ.

К примеру, современным банкам соответствие стандартам информационной безопасности навязывается извне регуляторами, такими как ЦБ РФ в случае с СТО БР ИББС (Стандарт Банка России по обеспечению информационной безопасности организаций банковской системы Российской Федерации) [2], PCI DSS – Payment Card Industry Data Security Standard — стандарт безопасности данных индустрии платёжных карт, разработанный Советом по стандартам безопасности индустрии платежных карт (Payment Card Industry Security Standards Council, PCI SSC) [3]. К коммерческим компаниям тоже может быть применен стандарт PCI DSS в случае работы с платежными шлюзами и т.п., Кроме того, могут применяться стандарты безопасности от NIST [4], ФСБ, ФСТЭК.

Большинство стандартов ИБ упомянутых выше являются высокоуровневыми и не содержат в себе спецификации, применяемые непосредственно к информационным системам. В таком случае на помощь приходят документы CIS, NIST и аналогичные.

Для США и Европы классификаторы стандартов и требований уже существуют. UCF (Unified Compliance Framework) [5] используется во многих современных GRC-продуктах. [6]

2 Применение стандартов информационной безопасности

Технически не очень сложно сформировать на основе высокоуровневого стандарта список требований к информационным системам, которые позволят повысить безопасность ИС. К примеру, многие стандарты ИБ призывают и регламентируют использование сложных и комплексных паролей, устанавливают политики смены их. В большинстве случаев, соответствие одному из стандартов информационной безопасности ведет к частичному соответствию и другому стандарту.

Таблица 1. Требование к паролям: PCI DSS

«В соответствии с данным требованием в паролях и (или) парольных фразах должно быть не менее семи символов (и букв, и цифр). Если данное минимальное требование не может быть выполнено в силу технических ограничений, организации могут рассмотреть альтернативные решения «эквивалентной надежности». Для дополнительной информации о вариативности и эквивалентной надежности (также используется термин «энтропия») паролей и (или) парольных фраз разных форматов следует обратиться к отраслевым стандартам (например, текущая версия NIST SP 800-63).» [7]

Основываясь на всем вышесказанном, определим алгоритм приведения стандартов к взаимосвязи или маппингу требований, что позволит нам построить сравнительные таблицы соответствия стандартам информационной безопасности.

Сначала требуется разложить высокоуровневый стандарт на технические и нетехнические требования. Возможность технически и централизованно проверить парольную политику явно будет относиться к технически проверяемым требованиям, размер лог-файла в операционной системе тоже явно технически проверяемые требования, а такое требование, как наличие стратегии информационной безопасности организации очень сложно будет проверить технически, и мы будем считать данную проверку нетехническим требованием.

Некоторые технически проверяемые требования могут быть сложно определяемы без контекста использования. Ярким примером является требование № 1.1.4 Стандарта PCI DSS – *«Требования о необходимости межсетевого экранирования каждого Интернет-соединения и соединений между каждой демилитаризованной зоной и внутренней сетью»* [5]. Для того, чтобы проверить соответствие данному требованию нужно определить наличие DMZ, правил сетевого экрана явно соответствующим схеме сети, а не просто проверить, запущена ли служба межсетевого экрана с правилами по умолчанию «Разрешить все».

Профилем стандартов будем называть совокупность технически проверяемых требований прямо или косвенно описываемых в стандартах ИБ. Профиль стандартов представим в виде JSON-файла с описанием пунктов стандарта и связей между технически определяемыми требованиями, операционными системами к которым данные рекомендации стандарта применимы, ссылками на аналогичные требования других стандартов.

Понятие «проверка соответствия» применимо не только для высокоуровневых и руководств NIST, но и для внутренних политик компаний. Многие требования корпоративных политик состоят из требований стандартов. Это означает, что можно выделить технические требования из стандартов, описанных в корпоративной политике ИБ, объединить их в политику и отслеживать соответствие профилю ИБ.

Высокоуровневые стандарты предполагают сбор и хранение информации об определенных событиях (указаны в таблице 2).

Таблица 2. Соотношение требований в стандартах [6]

	SOX	GLBA	FISMA	PCI DSS	HIPAA	ISO 2700x
Object Access	+		+	+	+	+
Logon	+	+	+	+	+	+
Policy Changes	+			+		+
System Events	+	+		+	+	+
Process Tracking	+					
Account Logon	+					+
User Access	+		+	+	+	+
Account Management	+					+
Security Assessment			+			+
Contingency Planning			+			+
Configuration Management			+	+		+

3 Автоматизированные средства проверки безопасности

Для автоматизации тестирования информационных систем используются модули в различных сканерах уязвимостей, как части проверок ИБ. К наиболее известным сканерам такого типа относятся, например, продукты компании Positive Technologies – MaxPatrol 8, MaxPatrol SIEM, компаний Tenable - Nessus Professional Vulnerability Scanner, различные GRC продукты.

В данной статье мы рассмотрим проект с открытым исходным кодом – SCAP Workbench [9], как основу функционального анализа для проектируемых систем автоматизации проверки соответствия стандартам информационной безопасности, где протокол автоматизации управления данными безопасности (SCAP) представляет собой набор открытых стандартов, определяющих технические спецификации для представления и обмена данными по безопасности. Эти данные могут быть использованы для нескольких целей, включая автоматизацию процесса поиска уязвимостей, оценки соответствия технических механизмов контроля и измерения уровня защищенности.

SCAP состоит из следующих стандартов:

- Типовые уязвимости и ошибки конфигурации (Common Vulnerabilities and Exposures CVE)
- Список типовых конфигураций (Common Configuration Enumeration CCE)
- Список типовых платформ (Common Platform Enumeration CPE)
- Единая система определения величины уязвимостей (Common Vulnerability Scoring System CVSS)
- Расширяемый формат описания списка проверки конфигурации (Extensible Configuration Checklist Description Format XCCDF)[10].
- Открытый язык описания уязвимостей и оценки (Open Vulnerability and Assessment Language OVAL)

Среди всего перечисленного рассмотрим расширяемый формат описания списка проверки конфигурации (XCCDF), который используем как основу при построении профилей стандартов.

XCCDF — это язык спецификаций для написания контрольных списков безопасности, контрольных показателей и связанных с ними видов документов. Документ XCCDF представляет собой структурированный набор правил настройки безопасности для некоторого набора целевых систем. Спецификация предназначена для поддержки обмена информацией, генерации документов и оценки соответствия. Спецификация также определяет модель данных и формат для хранения результатов тестирования контрольных показателей. Цель XCCDF заключается в том, чтобы обеспечить единую основу для выражения контрольных списков безопасности, контрольных показателей и других рекомендаций по настройке и тем самым способствовать более широкому применению эффективных методов обеспечения безопасности. [8]

В состав SCAP Workbench входит большое количество готовых файлов проверок, например для CentOS Linux 7 доступны следующие профили:

- C2S (государственные коммерческие облачные сервисы США) для CentOS Linux 7

- Политика безопасности информационных систем уголовного правосудия (CJIS)
- Общий профиль для систем общего назначения
- Стандартный профиль безопасности Docker-хостов
- Неклассифицированная информация в не федеральных информационных системах и организациях (NIST 800-171)
- Базовый уровень конфигурации правительства Соединенных Штатов (USGCB / STIG)
- PCI-DSS v3 Контрольная база для CentOS Linux 7
- Корпоративный профиль Red Hat для сертифицированных поставщиков облачных услуг (RH CCP)
- DISA STIG для CentOS Linux 7
- STIG для гипервизоров виртуализации Red Hat

Внешний вид программы представлен на рис. 1

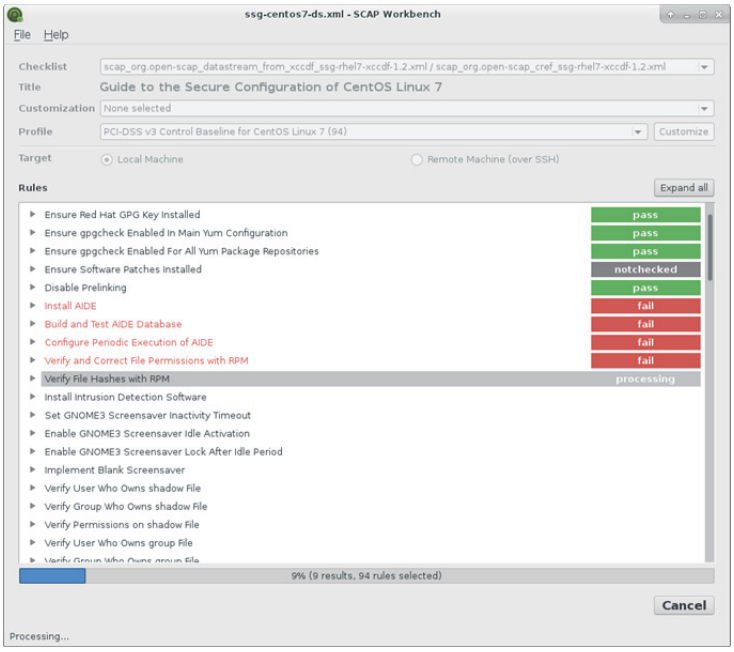

Рисунок 1 – Интерфейс SCAP Workbench

Для работы с профилями стандартов переведем XML-нотацию правил проверок в JSON-формат, как наиболее удобный формат для работы с данными.

На сайте http://json.org перечисляются некоторые преимущества JSON по сравнению с XML, в частности важно, что JSON легче для понимания и людьми, и машинами, поскольку его синтаксис минимален, а структура предсказуема. Кроме того, называется ещё одно большое преимущество JSON: то, что он изначально разработан как формат обмена структурированной информацией между программными продуктами и информационными системами.

К тому же мы внедряем дополнительные теги соответствия между стандартами информационной безопасности, что ведет к расширению и преобразованию XCCDF.

На рисунках 2 и 3 предоставлен фрагмент файла профиля безопасности PCI DSS – ssg-rhel7-xccdf.xml. В первом случае это XML-нотация, а во втором фрагмент преобразован в нотацию JSON.

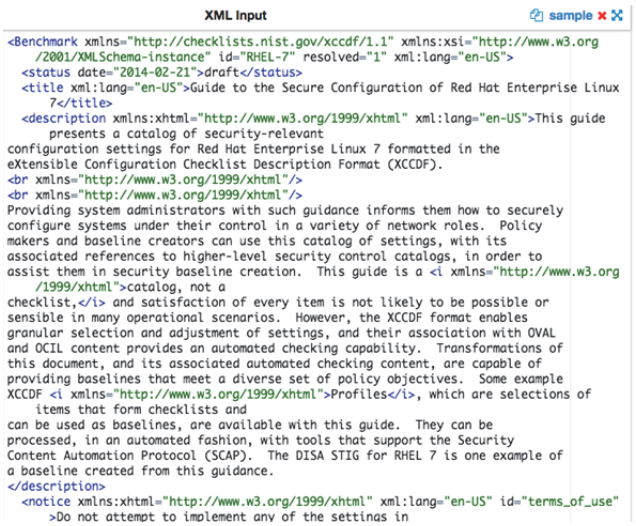

Рисунок 2 – Вид стандарта в XML-формате

Рисунок 3 – Вид стандарта в JSON-формате

Дополнительная очистка и преобразование XML, доработка соответствия различным стандартам будет произведена при формировании файлов профилей ИБ в ходе дальнейшей реализации предложенного подхода.

4 Заключение

В данной статье рассмотрены основные моменты по переработке высокоуровневых стандартов ИБ в технические требования, рассмотрен формат XCCDF как основа формирования профилей информационной безопасности и формирования маппинга требований ИБ и взаимосвязей стандартов между собой.

Маппинг требований стандартов информационной безопасности и переложение их на технические требования позволит компаниям построить систему управления информационной безопасности (СУИБ) на основе всестороннего анализа требований внешних регуляторов и стандартов ИБ. Оптимизация бизнес-процессов управления ИБ позволит обеспечивать должный уровень информационной безопасности, снижение влияния человеческого фактора и получения информации о безопасности систем почти в реальном времени. К тому же это позволит узнать по каким критериям мы уже соответствуем стандартам безопасности, что требуется доработать для усиления безопасности компании.

Внедрение различных профилей безопасности на основе профиля стандартов позволит автоматизированно проходить аудиторские проверки по информационной безопасности, так как вся информация по соответствию будет доступна в едином интерфейсе соответствующего программного инструментария, разработка которого ведётся на основе предложенного подхода.

Список использованной литературы:

[1] Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации" [Электронный ресурс] – URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=208191&fld=134&dst=100012,0&rnd=0.2327141976435436 2#06096376622461368 – 15.08.2018

[2] СТО БР ИББС [Электронный ресурс] – URL: https://ru.wikipedia.org/wiki/СТО_БР_ИББС – 15.08.2018

[3] PCI DSS [Электронный ресурс] – URL: https://ru.wikipedia.org/wiki/PCI_DSS – 15.08.2018

[4] NIST [Электронный ресурс] – URL https://ru.wikipedia.org/wiki/Национальный_институт_стандартов_и_технологий – 16.08.2018

[5] UCF [Электронный ресурс] – URL: http://www.unifiedcompliance.com – 16.08.2018

[6] Что такое GRC и чем это может быть полезно для ИБ? [Электронный ресурс] – URL: http://itsec.ru/articles2/control/chto-takoe-grc-i-chem-eto-mojet-bit-polezno-dlya-ib/ – 15.08.2018

[7] Стандарт безопасности данных индустрии платежных карт (PCI DSS). Требования и процедуры оценки безопасности Версия 3.2 Апрель 2016 г.

[8] Соответствие стандартам и политикам в сканерах уязвимостей и SIEM [Электронный ресурс] – URL: http://blog.ptsecurity.ru/2013/03/siem.html – 15.08.2018
[9] Assessing Linux Security Configurations with SCAP Workbench [Электронный ресурс] – URL: https://avleonov.com/2018/09/01/assessing-linux-security-configurations-with-scap-workbench/ – 30.08.2018
[10] Extensible Configuration Checklist Description Format (XCCDF) [Электронный ресурс] – URL: https://csrc.nist.gov/projects/security-content-automation-protocol/specifications/xccdf/ – 30.08.2018