УДК 004

СИСТЕМА МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА БАЗЕ ТРЕБОВАНИЙ PCI DSS И ISO/IEC 27001

Павлов К.А., Прихач И.В.

Белорусский национальный технический университет
Минск, Республика Беларусь

Существует множество стандартов по информационной безопасности. Среди них особо выделяют два, которые на данный момент весьма актуальны, схожи по масштабам своей распространенности и приняты на международном уровне. Это стандарты Payment Card Industry Data Security Standard (далее – PCI DSS) и ISO/IEC 27001.

Международный стандарт ISO/IEC 27001:2013 «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» разработан совместно Международной организацией по стандартизации и Международной электротехнической комиссией. Данный стандарт содержит требования для создания, внедрения, поддержания функционирования и непрерывного улучшения системы менеджмента информационной безопасности. Он применим по отношению к любым организациям (любого типа и размера). Внедрение и сертификация данной системы полностью добровольны. На данный момент действующей является версия 2013 года.

Стандарт PCI – стандарт безопасности данных для индустрии платежных карт. Он разработан Советом по стандартам безопасности индустрии платежных карт (далее – Совет PCI) и применяется исключительно к организациям, которые занимаются обработкой, хранением или передачей данных по платежным картам. Для подобных организаций выполнение требований стандарта является обязательным, однако, в зависимости от количества обрабатываемых карт, к таким организациям может применяться различный набор требований. С апреля 2016 года действует версия стандарта PCI DSS v. 3.2.

Несмотря на то, что оба стандарта освещают вопрос защиты информации, ISO/IEC 27001 является лучшим выбором для организаций, где уже существует какая-либо система менеджмента и которые хотят дополнить существующую систему в части защиты информации (или у которых нет системы менеджмента, но есть стремление к созданию подобной системы), в то время как PCI DSS более применим (и обязателен) для организаций, работающих с платежными картами.

В PCI DSS, в отличие от ISO/IEC 27001, существуют уровни соответствия для измерения уровня зрелости компании.

PCI DSS определяет 6 областей контроля и 12 основных требований по безопасности. Эти требования учтены в стандарте ISO/IEC 27001:2013 (табл. 1).

Таблица 1

Требование PCI DSS	Требование ISO/IEC 27001
1. Установка и обеспечение функционирования межсетевых экранов для защиты данных держателей карт	A.12 Безопасность производственной деятельности A.13 Безопасность обмена информацией
2. Неиспользование выставленных по умолчанию производителями системных паролей и других параметров безопасности	A.12 Безопасность производственной деятельности A.13 Безопасность обмена информацией
3. Обеспечение защиты данных держателей карт в ходе их хранения	A.12 Безопасность производственной деятельности A.13 Безопасность обмена информацией
4. Обеспечение шифрования данных держателей карт при их передаче через общедоступные сети	A.14 Приобретение, разработка и обслуживание систем
5. Использование и регулярное обновление антивирусного программного обеспечения	A.14 Приобретение, разработка и обслуживание систем
6. Разработка и поддержка безопасных систем и приложений	A.14 Приобретение, разработка и обслуживание систем
7. Ограничение доступа к данным держателей карт в соответствии со служебной необходимостью	A.12 Безопасность производственной деятельности A.13 Безопасность обмена информацией
8. Присвоение уникального идентификатора каждому лицу, имеющему доступ к информационной инфраструктуре	A.12 Безопасность производственной деятельности A.13 Безопасность обмена информацией
9. Ограничение физического доступа к данным держателей карт	A.11 Физическая безопасность и защита от природных угроз
10. Контроль и отслеживание всех сеансов доступа к сетевым ресурсам и данным держателей карт	A.12 Безопасность производственной деятельности A.13 Безопасность обмена информацией
11. Регулярное тестирование систем и процессов обеспечения безопасности	A.6 Организация информационной безопасности A.14 Приобретение, разработка и обслуживание систем A.18 Соответствие
12. Разработка, поддержка и исполнение политики информационной безопасности	A.5 Политики информационной безопасности

Соответствие требованиям стандарта PCI DSS должно оцениваться специалистом, обладающим статусом квалифицированного аудитора (буквально – оценщика) безопасности (Qualified Security Assessor – QSA), а также посредством автоматизированного ASV-сканирования уязвимостей периметра сети в заранее определенное и утвержденное Советом PCI время. В дальнейшем аудитор (буквально – оценщик) внутренней безопасности (Internal Security Assessor – ISA) может проводить самооценку организации посредством заполнения листа самооценки (SAQ), форма и наполнение которого зависит от размера и присвоенного по итогам проверки уровня организации.

Так, если организация претендует или ей ранее был присвоен уровень 1, то требования к ее сертификации включают:

– годовой отчет о соответствии (ROC) (ежегодный QSA аудит на месте);

– ежеквартальное ASV-сканирование;

– аттестацию соответствия (AOC).

На уровнях 2-4 ежегодный QSA аудит заменяет ежегодная самооценка посредством SAQ.

Стандарт ISO/IEC 27001 включает семь основных разделов в соответствии с Приложением SL (Annex SL). Использование тех же наименований разделов, что предложены Приложением SL, удобно для тех организаций, которые решили использовать единую систему менеджмента, которая соответствует требованиям двух или более стандартов систем менеджмента. Стоит заметить, что в тексте ISO/IEC 27001 не упоминается цикл Plan-Do-Check-Act (PDCA) напрямую, однако наименования разделов позволяют легко его расписать в контексте системы менеджмента. PCI DSS не включает в себя цикл PDCA.

Стандарт ISO/IEC 27001 содержит 14 позиций по управлению и 114 средств их реализации.

Для наилучшего обеспечения информационной безопасности организации рекомендуется совмещать PCI DSS и ISO/IEC 27001 при создании системы менеджмента.

Средства управления в ISO/IEC 27001 являются рекомендациями, в то время как средства управления в PCI DSS являются обязательными. Таким образом, стандарт ISO/IEC 27001 является более «гибким» и применимым, нежели PCI DSS. Соответствовать требованиям ISO/IEC 27001 проще (легче). Сравнение двух стандартов представлено в таблице 2.

Таблица 2

Параметр	ISO/IEC 27001	PCI DSS
Разработчик	ИСО	Совет PCI
Гибкость	Высокая	Низкая
Область применения	Зависит от организации	Данные по платежным картам
Средства управления	Высокого уровня	Низкого уровня
Тип средств управления	«следует»	«обязан»
Число средств управления	114	224
Аудит	Раз в три года сертификационный аудит и ежегодная периодическая оценка	Четыре ASV-сканирования и ежегодный аудит на месте для уровня 1
Сертификация	Возможна для любой организации	Возможна для любой организации
Уровни соответствия	Нет	Да

Оба вышеуказанных стандарта направлены на защиту конфиденциальной или личной информации. Однако в августе 2019 года ИСО был принят новый стандарт – ISO/IEC 27701:2019 «Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines» («Методы обеспечения безопасности. Расширение ISO/IEC 27001 и ISO/IEC 27002 – менеджмент конфиденциальной (частной) информации. Требования и рекомендации (руководящие указания)»). Это первый международный стандарт занятый вопросами управления конфиденциальными данными, который предоставляет руководство по управлению деятельностью для организаций, которые несут ответственность за обработку личной (конфиденциальной) информации.

УДК 533.9.01

ИССЛЕДОВАНИЕ ВЕЛИЧИНЫ И ХАРАКТЕРА РАСПРЕДЕЛЕНИЯ ПЛАЗМЕННОГО ПОТЕНЦИАЛА В ПРИКАТОДНОЙ ОБЛАСТИ РАЗРЯДА С ЭФФЕКТОМ ПОЛОГО КАТОДА В ТРУБЧАТОМ ЭЛЕКТРОДЕ

Божко А.И.

Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь

Проведено исследование величины и характера распределения плазменного потенциала в прикатодной области разряда с эффектом полого катода в трубчатом электроде применительно к различным газам. Установлены зависимости распределения величины потенциала пространства в зависимости от положения зонда относительно катода.

Использование разряда с эффектом полого катода позволяет переходить на новые ресурсосберегающие технологические процессы, причем область применения этих техпроцессов чрезвы-