УДК 004.056 Вестник УрФО № 2(56) / 2025, с. 49–57

**Серегина Ю. Н., Ложкин Р. А.,
Афанасьева М. В, Баранкова И.И.**

DOI: 10.14529/secur250205

ПРИМЕНЕНИЕ КОНЦЕПЦИИ IOT SECURITY MATURITY MODEL ДЛЯ ОЦЕНКИ СООТВЕТСТВИЯ PCI DSS ВЕРСИИ 4.0.1 ПРОЦЕССИНГОВОГО ЦЕНТРА

Статья рассматривает применение концепции IoT Security Maturity Model для оценки соответствия PCI DSS версии 4.0.1 в процессинговом центре. Предложена иерархическая модель, учитывающая ключевые требования стандарта, может быть применена для оценки соответствия требованиям стандарта PCI DSS. Разработаны профили зрелости и 5-балльная шкала оценки. Методика помогает оценить текущий уровень соответствия и спланировать модернизацию системы безопасности.

Ключевые слова: *IoT Security Maturity Model, процессинговый центр, PCI DSS 4.0.1, практики, текущий профиль, целевой профиль, управление рисками.*

Seregina Y. N., Lozhkin R.A., Afanasyeva M. V., Barankova I.I.

APPLICATION OF IOT SECURITY MATURITY MODEL CONCEPT FOR ASSESSING PCI DSS VERSION 4.0.1 COMPLIANCE OF A PROCESSING CENTER

The article examines the application of the IoT Security Maturity Model con-cept for assessing compliance with PCI DSS version 4.0.1 in a processing center. A hierarchical model has been proposed, taking into account the key requirements of the standard, which can be used to evaluate compliance with PCI DSS. Maturity profiles and a 5-point assessment scale have been developed. The methodology helps assess the current level of compliance and plan the modernization of the security system.

Keywords: *IoT Security Maturity Model, processing center, PCI DSS 4.0.1, practices, current profile, target profile, risk management.*

Введение

В условиях возрастающей сложности технологий, применяемых в финансовом секторе, особенно при обработке, передаче и хранении платежных карт, расширяется поверхность для возможных кибератак. Отсутствие безопасных автоматизированных систем, соблюдение нормативных требований увеличивает поверхность атак и создает новые риски, что особенно критично для процессинговых центров, работающих с платежными транзакциями.

Финансовый сектор, в частности процессинговый центр играет ключевую роль в обеспечении безопасности платежных операций, обрабатывая данные держателей карт (ДДК), критичные аутентификационные данные (КАД), авторизуя транзакции и взаимодействуя с банками-эмитентами и эквайерами. В таких условиях киберугрозы могут повлиять на значимые бизнес-процессы. Любая уязвимость в может привести к компрометации данных, финансовым потерям и репутационным рискам.

Таким образом, актуальной задачей является выработка обоснованного подхода к управлению информационной безопасностью и грамотное инвестирование в механизмы защиты, соответствующие стандартам банковской безопасности и требованиям PCI DSS [1].

В 2019 году Kaspersky ICS CERT [2] в сотрудничестве с отраслевыми партнерами разработали и представили практическое руководство «IoT Security Maturity Model: Practitioner's Guide». Исходная модель ориентирована на безопасность интернета вещей, в данном материале была использована концепция данного руководства для оценки соответствия PCI DSS версии 4.0.1 процессингового центра.

Модель зрелости информационной безопасности строится на сравнении целевого и текущего профилей безопасности. Эти профили представляют собой оценки полноты реализации доменов, поддоменов и практик, иерархия которых представлена на рисунке 1.

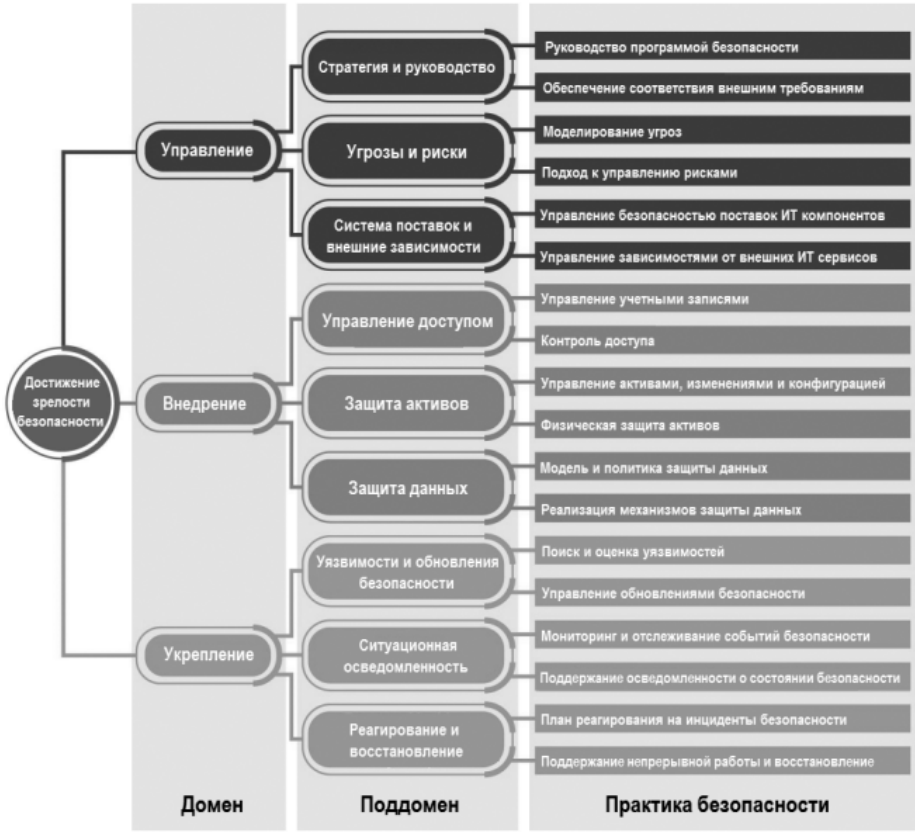

Рис. 1. Ранжирование доменов, поддоменов и практик в модели зрелости безопасности IoT Security Maturity Model: Practitioner's Guide

Целевой профиль зрелости отражает желаемое состояние системы защиты информации, к которому должна стремиться организация в процессе эксплуатации и поддержки своих информационных систем. Текущий профиль, напротив, демонстрирует реальное положение дел в области защиты данных. Каждый уровень модели зрелости оценивается по степени полноты реализации мер безопасности, которая зависит от объема применяемых практик, их систематичности и уровня обеспечиваемых гарантий.

Применение концепции IoT Security Maturity Model

PCI DSS является стандартом, регулирующим деятельность организаций, которые хранят, передают или обрабатывают данные держателей карт. Он состоит из 12 требований, определяющих ключевые принципы защиты платежных карт. В рамках данной работы была разработана модель зрелости для оценки соответствия PCI DSS версии 4.0.1 процессингового центра, где за домены взяты разделы стандарта, за практики – требования, а поддомены – проверочные процедуры, которые были сгруппированы по различным аспектам безопасности. Например, домен «Осуществлять регулярный мониторинг и тестирование сетей» разделяется на два поддомена «Контроль и мониторинг всего доступа к сетевым ресурсам и ДДК» и «Регулярное тестирование систем и процессов безопасности». Такое разделение было взято напрямую из стандарта. Само требование «Осуществлять регулярный мониторинг и тестирование сетей» было разделено на практики, которые были объединены в группы методом сравнения определенных требований подхода:

1. Процессы и механизмы регистрации и мониторинга всего доступа к компонентам системы и ДДК, куда входит проверочная процедура стандарта 10.1.

2. Журналы аудита надежно защищены и доступны, куда входит группа проверочных процедур стандарта 10.2–10.5.

3. Механизмы синхронизации времени поддерживаются во всех системах, куда входит проверочная процедура стандарта 10.6.

4. Сбои в критически важных системах контроля безопасности обнаруживаются, регистрируются и оперативно устраняются, куда входит проверочная процедура стандарта 10.7.

Полное ранжирование доменов, поддоменов и практик по стандарту PCI DSS версии 4.0.1 представлено на рисунке 2.

Существенные изменения в требованиях стандарта произошли за последнее время именно при переходе с версии 3.2.1 на 4.0. В новой редакции изменились как сами требования, так и подходы к их выполнению. На момент написания данной статьи актуальной версией PCI DSS является 4.0, однако в нем также описаны проверочные процедуры, которым с 31 марта 2025 года все организации, подлежащие сертификации, должны будут полностью соответствовать версии 4.0.1 [3]. В рамках использования концепции «IoT Security Maturity Model: Practitioner's Guide» для оценки соответствия PCI DSS версии 4.0.1 за текущий профиль зрелости были взяты требования версии 4.0 без учета новых проверочных процедур, а целевой профиль – полное соответствие требованиям стандарта, исходя из специфики бизнес-процессов [4]. Процессинговый центр проходил аудит именно в соответствии с обязательными проверочными процедурами на тот момент времени.

Модель зрелости безопасности процессингового центра по стандарту PCI DSS версии 4.0.1

При оценке текущего профиля зрелости безопасности учитывались проверочные процедуры стандарта PCI DSS. Ключевым фактором, влияющим на результат оценки, являлась специфика бизнес-процессов в процессинговом центре. Например, в рассматриваемой финансовой компании не применяются устройства POI. В свою очередь идеальная оценка строилась с учетом новых проверочных процедур, которые организации финансового сектора должны реализовать до 31 марта 2025 года. Шкала оценивания полноты представлена в списке:

- 0 – требование не применимо и обосновано бизнес-процессами;
- 1 – требование применимо, но не реализовано;
- 2 – требование применимо, но не реализовано в полной мере;
- 3 – требование полностью реализовано и соответствует построению бизнес-процессов в компании;
- 4 – требование полностью реализовано и построение бизнес-процессов соответствует наилучшим практикам стандарта PCI DSS.

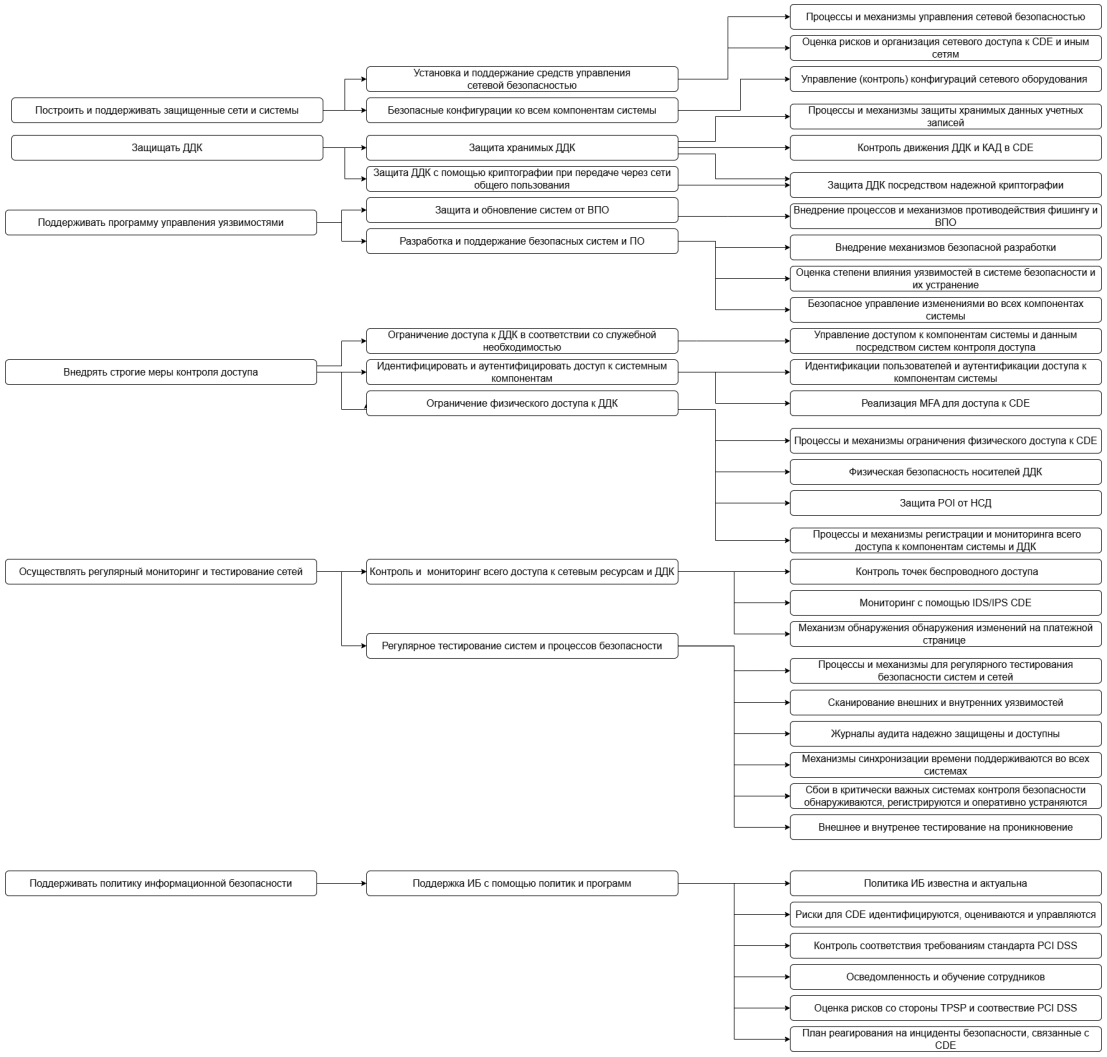

Рис 2. Ранжирование доменов, поддоменов и практик в модели зрелости, ориентированной на стандарт PCI DSS

Оценка полноты текущего профиля может иметь свое максимальное значение равное 3, поскольку новые требования уже прописаны в стандарте, но еще не реализованы в компании и будут обязательны только с 31 марта 2025 года и могут быть не реализованы в компании. Текущий профиль зрелости безопасности, а также его сравнение с целевым профилем, представлены на рисунке 3.

Организации необходимо распределить ответственность и обязанности за выполнение каждого требования стандарта, что напрямую влияет на практику «Осведомленность и обучение сотрудников». Требование выполняется методом фиксирования ролей и обязанностей, где используется матрица распределения ответственности, которая содержит данные о том, кто отвечает за выполнение задач и/или требований стандарта, кто подотчетен, с кем необходимо консультироваться и кого нужно информировать (также известная как матрица RACI).

При организации хранения ДДК необходимо учитывать все КАД, которые сохраняются до подтверждения транзакции. Защита таких данных обеспечивается применением современных криптографических алгоритмов в соответствии с требованиями стандарта PCI DSS, влияя на практику «Процессы и механизмы защиты хранимых данных учетных записей». Для сотрудников установлены строгие ограничения: запрещены любые манипуляции с ДДК при удаленной работе, за исключением специально уполномоченных лиц.

На практику «Защита ДДК посредством надежной криптографии» влияют проверочные процедуры:

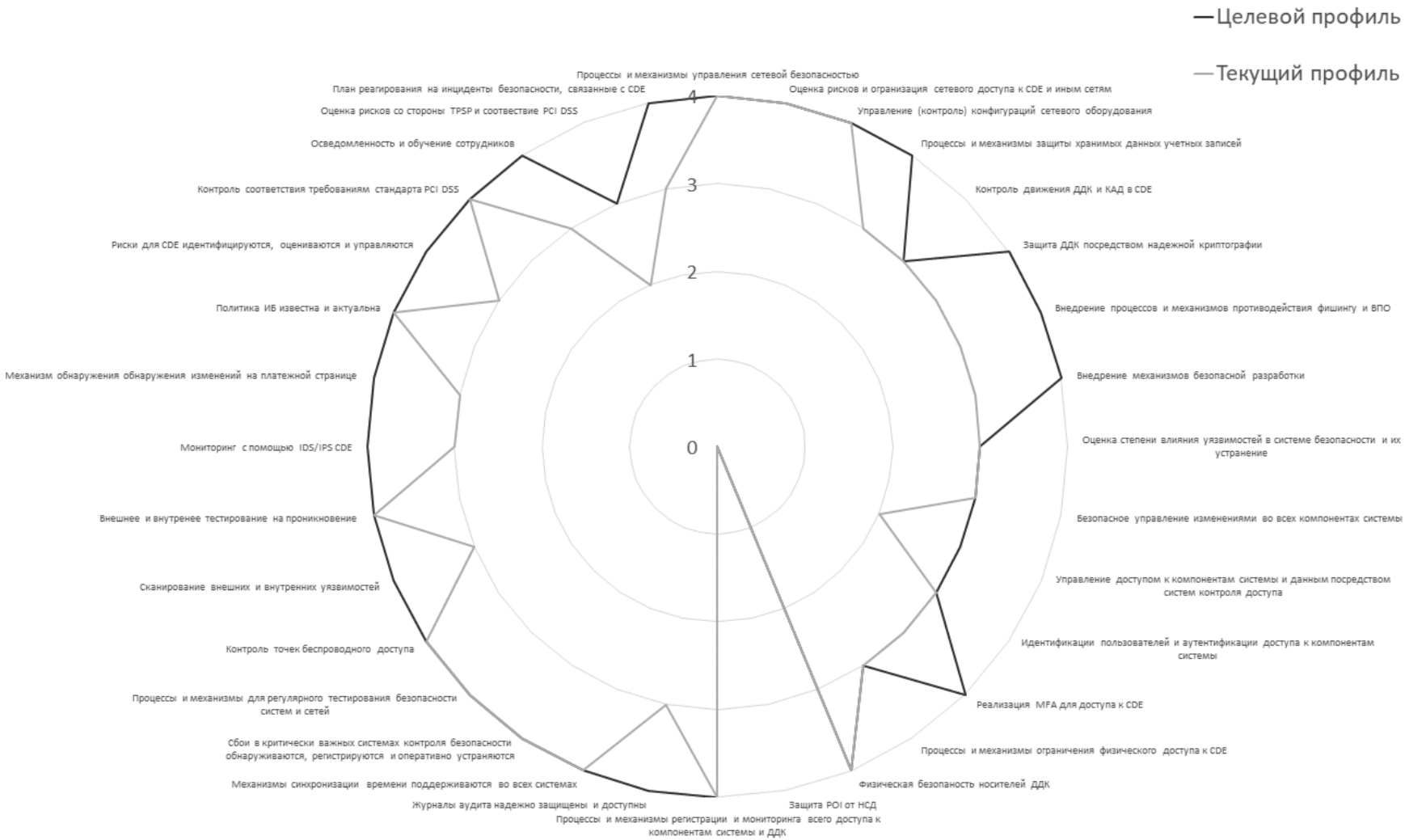

Рис. 3. Модель зрелости безопасности процессингового центра по стандарту PCI DSS версии 4.0.1

• Хеширования первичных учетных номеров (PAN) только с использованием хеш-функций с секретом.

• Процессы управления ключами должны соответствовать требованиям стандарта, изложенным в проверочных процедурах 3.6 и 3.7.

• Шифрование на уровне диска/разделов разрешено только для съемных носителей. В остальных случаях применяются методы, делающие PAN нечитаемым.

Рассматриваемый процессинговый центр ведет перечень доверенных ключей и сертификатов, используемых для защиты PAN при передаче, а также перечень используемого программного обеспечения (ПО) и его компонентов и перечень используемых криптографических протоколов, что влияет на практики «Защита ДДК посредством надежной криптографии», «Оценка степени влияния уязвимостей в системе безопасности и их устранение» и «Риски для CDE идентифицируются, оцениваются и управляются» соответственно.

В соответствии с требованиями стандарта PCI DSS, наилучшей практикой является автоматическое сканирование съемных носителей на предмет наличия вредоносного кода непосредственно при их подключении к системе. В качестве альтернативного подхода может применяться непрерывный мониторинг поведения системы и процессов при работе со съемными устройствами хранения данных. Параллельно организациям необходимо реализовать комплексные защитные механизмы, направленные на предотвращение фишинговых атак, с применением специализированных программных решений. Данные меры непосредственно способствуют реализации практики по противодействию фишингу и вредоносному программному обеспечению.

В соответствии с требованиями стандарта PCI DSS, критически важной практикой является автоматическое сканирование съемных носителей на предмет наличия вредоносного кода непосредственно при их подключении к системе. В качестве альтернативного подхода может применяться непрерывный мониторинг поведения системы и процессов при работе со съемными устройствами хранения данных. Параллельно организациям необходимо реализовать комплексные защитные механизмы, направленные на предотвращение фишинговых атак, с применением специализированных программных решений. Данные меры непосредственно способствуют реализации практики по противодействию фишингу и вредоносному программному обеспечению.

Особое внимание в новых требованиях уделяется обязательному применению межсетевого экрана уровня веб-приложений (WAF) для защиты публично доступных веб-ресурсов. В контексте защиты платежных страниц особую значимость приобретает использование политики безопасности контента (CSP), которая предполагает строгий контроль за исполняемыми скриптами. Каждый скрипт, выполняемый в браузере клиента, должен проходить процедуру авторизации, обладать гарантированной целостностью и быть зарегистрированным в системе учета с четким обоснованием его функционального назначения. Такой подход обеспечивает комплексную защиту платежных интерфейсов от потенциальных угроз.

В ежеквартальный аудит входит полная проверка всех учетных записей пользователей, что закрывает практику «Управление доступом к компонентам системы и данным посредством систем контроля доступа» и новые процедуры, связанные с учетными записями. Доступ к защищенной среде обработки данных держателей карт (CDE) организован с применением многофакторной аутентификации. Система аутентификации обладает устойчивостью к атакам повторного использования учетных данных, полностью исключая возможность их воспроизведения. При этом обход механизмов проверки невозможен ни для одной категории пользователей, включая администраторов системы, за исключением особых случаев, когда такое исключение официально санкционировано руководством на строго ограниченный период.

Процедура аутентификации построена на обязательном использовании как минимум двух независимых факторов подтверждения личности, что существенно повышает уровень защиты. Полноценный доступ к системе предоставляется исключительно после успешного прохождения всех предусмотренных этапов верификации, что гарантирует надежную защиту конфиденциальных данных от несанкционированного доступа. Такая реализация MFA обеспечивает комплексную безопасность CDE.

Важным изменением стало обязательное использование автоматизированных механизмов для проведения обзора журналов ау-

дита, что закрывает практику «Журналы аудита надежно защищены и доступны». Использование специализированных решений для мониторинга, включая SIEM-системы и анализаторы логов, существенно упрощает процесс обработки событий безопасности за счет автоматического выявления подозрительных записей в журналах. В компании внедрена SIEM система, что обеспечивает глубокий анализ инцидентов.

Стандарт PCI DSS 4.0.1 изменил подход к управлению рисками, сделав его более системным и интегрированным в процессы информационной безопасности. Основу нового подхода составляет требование 12.3.1, которое обязывает организации проводить регулярный целевой анализ рисков. Этот анализ становится основой для принятия ключевых решений в области безопасности: от определения периодичности пересмотра прав доступа до установки сроков действия паролей системных учетных записей. Данное требование напрямую влияет на практику «Риски для CDE идентифицируются, оцениваются и управляются».

Оценка практики «План реагирования на инциденты безопасности, связанные с CDE» также увеличила свою оценку благодаря учету инцидентов с нарушением целостности платежных страниц или HTTP-заголовков (требование 12.10.5), а также с обнаружением PAN в нерегламентированных местах хранения (требование 12.10.7). Данные инциденты включены в политику реагирования, что значительно влияет на безопасность ДДК и КАД.

Теперь внутренние сканирующие системы обязаны использовать авторизованный доступ с минимально необходимыми привилегиями, что значительно повышает оценку практики «Сканирование внешних и внутренних уязвимостей», так как обеспечивается более глубокое понимание ландшафта уязвимостей.

Заключение

Таким образом, новая версия стандарта содержит в себе ключевые изменения, помогающие процессинговому центру и иным компаниям финансового сектора поддерживать уровень защиты информации без негативного влияния на бизнес-процессы. Применение подходов IoT Security Maturity Model позволяет оценивать уровень готовности организации к переходу на новую версию стандарта PCI DSS. Данная концепция позволяет наглядно представить новые процедуры стандарта благодаря четкой иерархии и ранжированию требований стандарта. Модель зрелости безопасности дает понимание текущего состояния защиты финансовой организации, задает вектор развития и упрощает подготовку процессингового центра к аудите на соответствие требованиям стандарта PCI DSS.

Литература

1. Стандарт безопасности данных индустрии платежных карт (PCI DSS) версия 4.0 [Электронный ресурс] / SecurITM — Электрон. дан. — Режим доступа: https://service.securitm.ru/docs/pci-dss-v4-0-ru, свободный. — Загл. с экрана.

2. Консорциум индустрии интернета: практическое руководство по модели зрелости безопасности интернета вещей [Электронный ресурс] / IIC — Электрон. дан. — 2020. — Режим доступа: https://www.iiconsortium.org/pdf/IoT_SMM_Practitioner_Guide_2020-05-05.pd, свободный. — Загл. с экрана.

3. Отличия требований PCI DSS версии 4.0 от версии 3.2.1 [Электронный ресурс] / Deiteriy Compliance — Электрон. дан. — Режим доступа: https://compliance.deiteriy.com/pci_dss_requirements_differences, свободный. — Загл. с экрана.

4. Федорова, А. Р. Модель зрелости безопасности промышленного интернета вещей / А. Р. Федорова, О. А. Казаков, М. В. Афанасьева // Актуальные проблемы современной науки, техники и образования: Тезисы докладов 79-й международной научно-технической конференции, Магнитогорск, 19–23 апреля 2021 года. Том 1. – Магнитогорск: Магнитогорский государственный технический университет им. Г.И. Носова, 2021. – С. 403.

5. Баранкова И. И. Построение модели зрелости информационной безо-пасности для АСУ ТП ЦППН / И. И. Баранкова, М. В. Афанасьева, А. В. Дегтярева // Вестник УрФО. Безопасность в информационной сфере. – 2022. – № 2(44). – С. 57-62. – DOI 10.14529/secur220208.

References

1. Standart bezopasnosti dannykh industrii platezhnykh kart (PCI DSS) versiya 4.0 [Elektronnyy resurs] / SecurITM — Elektron. dan. — Re-zhim dostupa: https://service.securitm.ru/docs/pci-dss-v4-0-ru, svobodnyy. — Zagl. s ekrana.

2. Konsortsium industrii interneta: prakticheskoye rukovodstvo po mo-deli zrelosti bezopasnosti interneta veshchey [Elektronnyy resurs] / IIC — Elektron. dan. — 2020. — Rezhim dostupa: https://www.iiconsortium.org/pdf/IoT_SMM_Practitioner_Guide_2020-05-05.pd, svobodnyy. — Zagl. s ekrana.

3. Otlichiya trebovaniy PCI DSS versii 4.0 ot versii 3.2.1 [Elektron-nyy resurs] / Deiteriy Compliance — Elektron. dan. — Rezhim dostupa: https://compliance.deiteriy.com/pci_dss_requirements_differences, svobodnyy. — Zagl. s ekrana.

4. Fedorova, A. R. Model' zrelosti bezopasnosti promyshlennogo in-terneta veshchey / A. R. Fedorova, O. A. Kazakov, M. V. Afanas'yeva // Aktual'-nyye problemy sovremennoy nauki, tekhniki i obrazovaniya: Tezisy dokladov 79-y mezhdunarodnoy nauchno-tekhnicheskoy konferentsii, Magnitogorsk, 19–23 aprelya 2021 goda. Tom 1. – Magnitogorsk: Magnitogorskiy gosudarstven-nyy tekhnicheskiy universitet im. G.I. Nosova, 2021. – S. 403.

5. Barankova I. I. Postroyeniye modeli zrelosti informatsionnoy bez-opasnosti dlya ASU TP TSPPN / I. I. Barankova, M. V. Afanas'yeva, A. V. Degtyareva // Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. – 2022. – № 2(44). – S. 57-62. – DOI 10.14529/secur220208.

БАРАНКОВА Инна Ильинична, доктор технических наук, доцент, за-ведующая кафедрой информатики и информационной безопасности, ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: inna_barankova@mail.ru.

АФАНАСЬЕВА Маргарита Владимировна, старший преподаватель кафедры информатики и информационной безопасности, ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: nansy_stokli@mail.ru.

СЕРЕГИНА Юлия Николаевна, студент кафедры информатики и ин-формационной безопасности, ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: pip_p@internet.ru.

ЛОЖКИН Роман Александрович, студент кафедры информатики и ин-формационной безопасности, ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: roman_2001@icloud.com.

BARANKOVA Inna Ilyinichna, Doctor of Technical Sciences, Associate Professor, Head of the Department of computer science and information security, Federal State Budgetary Educational Institution of Higher Education "Magnitogorsk State Technical University named after G.I. Nosov". 455000, Magnitogorsk, Lenin Ave., 38. E-mail: inna_barankova@mail.ru.

AFANASYEVA Margarita Vladimirovna, Assistant Professor of the Department of computer science and information security, Federal State Budgetary Educational Institution of Higher Education "Magnitogorsk State Technical University named after G.I. Nosov". 455000, Magnitogorsk, Lenin Ave., 38. E-mail: nansy_stokli@mail.ru.

SEREGINA Yulia Nikolaevna, student of the Department of computer science and information security, Federal State Budgetary Educational Institution of Higher Education "Magnitogorsk State Technical University named after G.I. Nosov". 455000, Magnitogorsk, Lenin Ave., 38. E-mail: pip_p@internet.ru.

LOZHKIN Roman Alexandrovich, student of the Department of computer science and information security, Federal State Budgetary Educational Institution of Higher Education "Magnitogorsk State Technical University named after G.I. No-sov". 455000, Magnitogorsk, Lenin Ave., 38. E-mail: roman_2001@icloud.com.