DOI: 10.18372/2410-7840.21.14337
УДК 004.056

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МОДЕЛЕЙ ОЦЕНКИ ЗРЕЛОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Михаил Коломыцев, Светлана Носок, Роман Тоцкий

Информационная безопасность может быть определена как: защита информационных активов посредством обработки рисков, направленных на нарушение конфиденциальности, целостности и доступности информации, которая обрабатывается, хранится и передается между взаимосвязанными информационными системами; и процесс, который включает предотвращение, обнаружение и реакцию на угрозы информационной безопасности. В мировой практике для определения стадии организационного и технологического развития организации и её процессов применяется понятие модели зрелости. Для измерения состояния процесса используется набор метрик, которые представляют собой определенные характеристики. Оценивание этих метрик по установленной шкале показывает состояние процессов, которое и будет характеризовать уровень их зрелости. В мировой практике, в отличие от украинской, применение модели зрелости для управления процессами информационной безопасности широко распространено. Примером этого может служить серия стандартов ISO27000, которая регулирует вопросы управления информационной безопасностью, реализуемых на основе Системы Управления Информационной Безопасностью. Очевидно, что перед организацией, осуществляющей деятельность по управлению информационной безопасности, рано или поздно встает вопрос о том, как выполнять эти требования, в каком объеме и на каком уровне детализации и т.п. Ответить на эти и другие вопросы может помочь модель зрелости, на основе которой будет проводится оценка уровня зрелости процессов информационной безопасности. Для определения основных моделей зрелости информационной безопасности был проведен анализ открытых источников и лучших практик, связанных с моделями зрелости информационной безопасности. На основании результатов анализа источников были определены наиболее применимые модели зрелости информационной безопасности, а именно: SSE-CMM, C2M2, NICE и O-ISM3.

Ключевые слова: *информационная безопасность; модель зрелости;ISO 27001; СУИБ; сравнительный анализ; метрики.*

1. АКТУАЛЬНОСТЬ И ПОСТАНОВКА ЗАДАЧИ

Цель данной статьи – описать и сравнить наиболее используемые модели зрелости информационной безопасности для анализа их соответствия целям использования совместно с стандартом ISO 27001. В статье показано, что модели зрелости информационной безопасности имеют схожие элементы, домены и уровни зрелости. Они также основываются на оценке рисков, хотя и на разных уровнях глубины. Было отмечено, что каждая модель в силу своей специфики имеет различные области применения.

Зрелость информационной безопасности организации определяется набором показателей, характеризующих способность организации соответствовать текущим и будущим вызовам нарушений информационной безопасности. Уровень зрелости показывает, насколько процесс обеспечения информационной безопасности управляем и прогнозируем.

Особенностью данного процесса является то, что он включает в себя технологии, людей, и процедуры (процессы), обеспечивающих комплексный подход к обеспечению информационной безопасности, что достигается путем внедрения ведущих практик.

Чтобы организации могли улучшить свои методы обеспечения информационной безопасности, отраслевые и технические сообщества были разработаны модели зрелости информационной безопасности, которые позволяют измерять текущее состояние защищенности организаций и позиционировать их на разных уровнях зрелости. Существуют различные модели зрелости, во многих случаях разработанные государственными структурами с целью стать национальными/международными стандартами, в дальнейшем дорабатывались коммерческими отраслевыми организациями для соответствия их конкретным потребностям.

Поэтому важно ответить на следующие вопросы:

– Каковы основные модели зрелости, используются для измерения состояния информационной безопасности?

– Каковы различия между основными моделями зрелости и есть ли возможность применять их для оценки зрелости Системы Управления Информационной Безопасностью (СУИБ), построенной по стандарту ISO 27001?

Ответ на эти вопросы является предметом данной статьи. Данное исследование проводится

с целью выявления основных отличий, преимуществ и недостатков моделей зрелости, наиболее часто используемых для оценки информационной безопасности, и дальнейшей разработки модели зрелости, которая может использоваться организацией для формирования стратегии развития собственной функции информационной безопасности.

В разделе 2 представлена концепция модели зрелости информационной безопасности; в разделе 3 - методология сравнительного исследования и особенности сравнения моделей зрелости информационной безопасности; раздел 4 показывает описание и структуру моделей зрелости информационной безопасности; раздел 5 показывает результаты, полученные из сравнения; и в разделе 6 приведены выводы, полученные из сравнительного анализа моделей зрелости информационной безопасности.

2. МОДЕЛИ ЗРЕЛОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Модель зрелости основана на процессной модели улучшения. Первая такая модель была разработанна Институтом разработки программного обеспечения (SEI) в середине 1980-х годов. Процессная модель - это структурированная совокупность практик, которые описывают характеристики эффективных процессов. Эта концепция также применяется к моделям зрелости с учетом процессов, связанных с информационной безопасностью [1].

Таким образом, модель зрелости информационной безопасности обеспечивает эталон, с помощью которого организация может оценить текущий уровень зрелости своих процессов и практик, установить цели и приоритеты для улучшения уровня информационной безопасности. Модели зрелости информационной безопасности обычно структурированы по следующим элементам:

– Домены: домены группируют в себе общие концепции организационных процессов, и каждый домен не обязательно независим от других.

– Уровни зрелости: это результат оценки выполнения факторов и показателей в доменах или измерениях организации. Уровни зрелости варьируются от начального уровня, на котором организация, возможно, только начала рассматривать информационную безопасность, до оптимизируемого, где организация способна быстро адаптироваться к изменениям в ландшафте угроз, уязвимостей, рисков информационной безопасности или изменениям внутри организации.

Для определения основных моделей зрелости информационной безопасности был проведен анализ открытых источников и лучших практик, связанных с моделями зрелости информационной безопасности [2, 3].

На основании результатов анализа источников были определены наиболее применимые модели зрелости информационной безопасности, а именно: SSE-CMM (The Systems Security Engineering Capability Maturity Model) [4], C2M2 (Cybersecurity Capability Maturity Model)[5], NICE (The National Initiative for Cybersecurity Education)[6] и O-ISM3 (Open In formation Security Management Maturity Model)[7].

Были найдены другие модели зрелости, но они не были рассмотрены в этом исследовании, потому что не подходили по критерию применимости для оценки зрелости информационной безопасности. Некоторые из моделей, которые не были рассмотрены: COBIT (Control Objectives for Information and Related Technologies) и BSIMM (The Building Security In Maturity Model). COBIT - это модель, которая не решает проблему информационной безопасности, а фокусируется на управлении ИТ. BSIMM- это модель, помогающая понять и спланировать инициативы по безопасности разрабатываемого ПО, что является лишь одной из задач информационной безопасности.

3. МЕТОДОЛОГИЯ, ИСПОЛЬЗУЕМАЯ ДЛЯ ПРОВЕДЕНИЯ СРАВНИТЕЛЬНОГО АНАЛИЗА

По результатам предыдущего анализа были определены наиболее подходящие модели оценки зрелости, а именно: SSE-CMM, C2M2, NICE, O-ISM3.

Для проведения сравнительного анализа моделей зрелости были определены следующие критерии:

– Ориентированность на информационную безопасность: может ли модель быть применена для оценки зрелости информационной безопасности. Этот критерий является фундаментальным для рассмотрения того, какие модели были разработаны для оценки зрелости информационной безопасности, а какие нет.

– Применимость к СУИБ: может ли модель быть применена для оценки зрелости СУИБ. Этот критерий позволяет ответить на вопрос возможности применения для оценки зрелости СУИБ, построенной согласно стандарту ISO 27001.

– Год последнего пересмотра: последний пересмотр модели. Этот критерий может предоста-

вить информацию об актуальности модели и способности соответствовать постоянным изменениям в информационной безопасности.

– Полнота применения: модель зрелости ориентирована на всю организацию или нет. Этот критерий предоставляет информацию о том, была ли модель зрелости создана для оценки информационной безопасности в целом для всех организаций, или фокусируется на определенных областях.

– Глубина: зависит от сложности используемой проверки. Этот критерий позволяет определить различие между моделями, которые имеют большую детализацию в соответствующих уровнях зрелости, и моделями, которые являются простыми в этом аспекте.

– Уровень документации для реализации: насколько имеющаяся документация помогает в реализации модели. Таким образом, можно определить, на каком уровне детализации имеется информация для реализации модели.

Каждый критерий был оценен следующим образом:

– Ориентированность на информационную безопасность. Эта функция оценивается как «ДА», если это модель, ориентированная на информационную безопасность, и как «НЕТ» в противном случае.

– Применимость к СУИБ. Эта функция оценивается как «ДА», если это модель, применима к СУИБ, и как «НЕТ» в противном случае.

– Год последнего пересмотра. В этой функции оценивается последний год обзора, чем новее, тем лучше.

– Полнота применения. Если модель ориентирована на всю организацию, критерий оценивается как «ДА». В случае, если он ориентирован на конкретную область организации, он оценивается как «НЕТ».

– Глубина. Этот критерий оценивается как «ОБЩАЯ», если в пределах уровней зрелости существует только верхнеуровневая оценка. Он оценивается как «УГЛУБЛЕННАЯ», если модель имеет определенную углубленность уровней оценки зрелости.

– Уровень документирования для реализации. Уровень документирования считается «ВЫСОКИМ», если есть официальный документ, руководство по внедрению и сопутствующие документы. Уровень документирования считается «СРЕДНИМ», если у модели есть официальный документ и сопутствующие документы. Уровень документирования считается «НИЗКИМ», если он имеет только обзорные вступительные документы.

4. СРАВНЕНИЕ ВЫБРАННЫХ МОДЕЛЕЙ ЗРЕЛОСТИ

В этом разделе описаны основные компоненты и структура моделей зрелости, которые ориентированы на информационную безопасность, и те, которые были адаптированы для оценки информационной безопасности.

4.1. Модель зрелости C2M2

Министерство энергетики США в сотрудничестве с Университетом Карнеги-Меллона опубликовало модель зрелости информационной безопасности. Последняя версия (1.1) модели была опубликована в феврале 2014 года.

Модель состоит из десяти доменов, и каждый домен представляет собой логическую группу практик кибербезопасности. Практики в каждой области организованы в цели, которые представляют достижения в области. Домены и практики перечислены в таблице 1.

Модель определяет четыре уровня зрелости, от уровня 0 до уровня 3, которые применяются независимо к каждой области модели. Описание каждого уровня приведено в таблице 2.

Модель C2M2 обеспечивает описательное, а не предписывающее руководство. Содержание модели представлено на высоком уровне абстракции, так что ее могут интерпретировать организации различных типов, структур и размеров.

4.2. Модель зрелости SSE-CMM

Первоначально разработку модели финансировало Агентство национальной безопасности США (АНБ). Первая версия модели была опубликована в октябре 1996 года, а последняя версия модели - в октябре 2008 года. Последний раз эта модель была пересмотрена в 2014, поэтому данная версия остается актуальной. SSE-CMM имеет два направления: «домен» и «возможности». Домен состоит из всех практик, которые в совокупности определяют проектирование информационной безопасности, и эти практики называются «базовыми практиками». Измерение возможностей представляет практики, которые указывают на управленческие возможности и институционализацию процесса, и эти практики называются «общими практиками». Общие практики представляют собой виды деятельности, которые следует выполнять как часть выполнения базовых практик. SSE-CMM содержит 129 базовых практик, организованных в 22 технологических областях. Из них 61 базовая практика, организованная в 11 областях процессов, охватывает все основные области проектирования информационной безопасности. Другие 68 базовых практик (организованных в других 11 областях процессов), связанных с Проектом и Организацией, показаны в таблице 3.

Таблица 1

Соответствие доменов и практик в модели MLS

Домены	**Практики**
Управление рисками	Разработать стратегию управления рисками кибербезопасности
	Управление рисками кибербезопасности
	Управленческая деятельность
Управление активами, изменениями и конфигурацией	Управление Инвентаризацией Активов
	Управление конфигурацией активов
	Управление изменениями в активах
	Управленческая деятельность
Управление идентификацией и доступом	Установка и поддерживать идентификаторы
	Контроль доступа
	Управленческая деятельность
Управление угрозами и уязвимостями	Выявление и реагирование на угрозы
	Уменьшить уязвимости кибербезопасности
	Управленческая деятельность
Мониторинг среды	Ведение журнала
	Выполнить мониторинг
	Создать и поддерживать общую рабочую картину
	Управленческая деятельность
Обмен информацией и связь	Обмен информацией о кибербезопасности
	Управленческая деятельность
Реагирование на события и инциденты, непрерывность операций	Обнаружение событий кибербезопасности
	Эскалация событий кибербезопасности и объявление инцидентов
	Реагировать на инциденты и эскалации
	Событий кибербезопасности
	План для непрерывности
	Управленческая деятельность
Управление цепочками поставок и внешними зависимостями	Определить зависимости
	Управление рисками зависимости
	Управленческая деятельность
Управление персоналом	Ответственность за кибербезопасность
	Контролировать жизненный цикл рабочей силы
	Разработка рабочей силы по кибербезопасности
	Повышение осведомленности о кибербезопасности
	Управленческая деятельность
Управление программой кибербезопасности	Установить стратегию программы кибербезопасности
	Спонсорская программа кибербезопасности
	Создание и поддержка архитектуры кибербезопасности
	Выполнить безопасную разработку программного обеспечения
	Управленческая деятельность

Таблица 2

Уровни зрелости в модели MLS

Уровень показателя зрелости (MIL)	**Описание уровня**
MIL 0	Модель не содержит практик для MIL0. Производительность в MIL0 просто означает, что MIL1 в данном домене не был достигнут.
MIL 1	В каждом домене MIL1 содержит набор начальных практик. Чтобы достичь MIL1, эти начальные действия могут быть выполнены специальным образом, но они должны быть выполнены.
MIL 2	Показатели деятельности организации более стабильны. На MIL2 организация может быть более уверена в том, что эффективность практики в области будет поддерживаться с течением времени.
MIL 3	На MIL3 практика в домене еще более стабилизируется и руководствуясь организационными директивами высокого уровня, такими как политика.

Таблица 3

Базовые практики в модели SSE-CMM

Проектирование информационной безопасности	**Проект и организация**
PA01 Управление средствами защиты	PA12 Обеспечение качества
PA02 Оценка воздействия	PA13 Управление конфигурацией
PA03 Оценка рисков безопасности	PA14 Управление рисками проекта
PA04 Оценка угроз	PA15 Мониторинг и управление техническойдеятельностью
PA05 Оценка уязвимостей	PA16 Планированиетехническойдеятельности
PA06 Формирование аргументов доверия	PA17 Определение процесса системного проектирования организации
PA07 Координация задач безопасности	PA18 Улучшение процесса системного проектирования организации
PA08 Мониторинг состояния безопасности	PA19 Управление линейкой развития производственных систем
PA09 Входные данные по безопасности	PA20 Управление средой поддержки системного проектирования
PA10 Обозначение потребностей в безопасности	PA21 Обеспечениепрактических навыков и знаний
PA11 Проверка и подтверждение безопасности	PA22 Сотрудничество с поставщиками

Базовые практики организованы в областях процессов, и каждая область процессов имеет ряд целей, которые представляют ожидаемое состояние процесса. Организация, которая выполняет базовые практики в области процессов, должна также достичь своих целей. Общие практики сгруппированы в логические области, называемые «Общими чертами», которые организованы в пять «уровней зрелости», которые представляют расширенные возможности организации. Общие функции предназначены для описания основных изменений в типичном способе организации рабочих процессов организации, и каждая общая функция имеет одну или несколько общих практик.

SSE-CMM имеет пять уровней зрелости, как показано в таблице ниже.

Таблица 4

Уровни зрелости SSE-CMM

Уровень зрелости	**Описание уровня**
Уровень 1, «Выполнено неформально»	Базовые практики области процесса обычно выполняются. Выполнение этих базовых практик не может быть строго спланировано и отслежено.
Уровень 2, «Запланировано и отслежено»	Выполнение базовых практик в области процессов планируется и отслеживается. Работоспособность в соответствии с указанными процедурами проверяется.
Уровень 3, «Хорошо определенные»	Базовые практики выполняются в соответствии с хорошо определенным процессом с использованием утвержденных, адаптированных версий стандартных, документированных процессов.
Уровень 4, «Количественно контролируемый	Подробные показатели эффективности собираются и анализируются. Это приводит к количественному пониманию возможностей процесса и улучшенной способности прогнозировать производительность.
Уровень 5, «Постоянно совершенствующийся»	Количественные цели (целевые показатели) эффективности и результативности процесса устанавливаются на основе бизнес-целей организации.

Описанная модель считается моделью, не ориентированной на информационную безопасность, но она была адаптирована организацией ISO для этой цели из-за отсутствия моделей, специфичных для информационной безопасности.

4.3. Модель зрелости NICE

Национальная образовательная инициатива по кибербезопасности (NICE) возникла из Инициативы по комплексной кибербезопасности (CNCI), которая была учреждена Президентом США Джорджем Бушем в Президентской директиве по национальной безопасности в январе 2008 года. Её целью было развивать персонал с технологическим профилем в кибербезопасности, с применением соответствующих знаний и навыков. Единственная версия (1.0) модели была опубликована в августе 2014 года.

Модель зрелости NICE разделяет ключевые виды деятельности на три основные области:

– Процесс и аналитика. Процесс представляет собой те действия, которые связаны с фактическими шагами, предпринимаемыми организацией для планирования рабочей силы, и тем, как эти шаги интегрированы с другими важными бизнес-процессами во всей организации. Аналитика представляет собой те виды деятельности, которые связаны с данными о спросе и предложении, а также с использованием инструментов, моделей и методов для анализа кадрового планирования.

– Интегрированное управление: представляет собой те виды деятельности, которые связаны с созданием структур управления, разработкой и предоставлением руководящих указаний, а также движением принятия решений. Это строительный блок для общей стратегии и видения планирования рабочей силы организации, а также распределения ответственности, содействия интеграции и выпуска руководства по планированию.

– Обученные профессионалы и вспомогательные технологии. Представляет деятельность, связанную с созданием профессиональных кадровых специалистов в организации. Вспомогательные технологии представляют деятельность, связанную с доступностью и использованием систем. Модель зрелости NICE имеет три уровня зрелости. Эти уровни показаны в таблице 5.

Таблица 5

Уровни зрелости в модели NICE

Уровень зрелости	**Описание уровня**
Ограниченный уровень	Ограниченный - самый базовый уровень, изображающий организацию с областями ее способности планирования рабочей силы. Эта ключевая область организации находится в начале своего развития, например, имеет ограниченную структуру процессов, не имеет четкого руководства.
Прогрессирующий уровень	Прогрессирующий уровень описывает некоторые аспекты планирования рабочей силы во всей организации, которая начала выполнять и создавать некоторую инфраструктуру для поддержки потребностей.
Оптимизированный уровень	Описывает ключевые области возможностей планирования рабочей силы в организации, которые полностью разработаны, интегрированы с другими бизнес-процессами и могут поддерживать различные уровни анализа, результаты которых способствуют принятию краткосрочных и долгосрочных решений для рабочей силы в области кибербезопасности.

4.4. МодельO-ISM3

Модель O-ISM3 описывает основные процессы управления информационной безопасностью, присущие большинству организаций. O-ISM3 разработан с учетом всех видов организаций. В частности, бизнес, неправительственные организации и предприятия, которые растут или аутсорсинг [8].

Задачами этого стандарта являются:

– Обеспечить подход к созданию систем управления информационной безопасностью (СУИБ), которые полностью соответствуют бизнес-целей и требованиям соответствия.

– Обеспечить подход, применимый к любой организации, независимо от ее размера, контекста и ресурсов.

– Предоставить организациям возможность определять приоритеты и оптимизировать свои инвестиции в информационную безопасность.

– Обеспечить постоянное улучшение СУИБ с использованием метрик.

– Включить управляемый метриками проверяемый аутсорсинг процессов безопасности.

Выделяются задачи процессов обеспечения информационной безопасности и метрики, непосредственно вытекающие из бизнес-целей организации. Отмечается, что каждый процесс обеспечения информационной безопасности вносит свой вклад в реализацию основных целей управления информационной безопасностью, которые определяются следующим образом:

– предотвращать и снижать число инцидентов информационной безопасности, которые могут поставить под угрозу активы организации, поставляемую ею продукцию и предоставляемые сервисы, основанные на использовании информационных систем;

– оптимизировать использование информации, финансов, людей, времени и инфраструктуры.

Основная идея стандарта O-ISM3 как стандарта по управлению информационной безопас-

ностью заключается в том, что её обеспечение связано не только с предотвращением атак на активы, но и с достижением в рамках установленного бюджета бизнес-целей организации, несмотря на различные возможные инциденты ИБ (атаки, технические сбои, ошибки персонала и т.д.).

Модель O-ISM3 оценивает зрелость функционирования существующих процессов СУИБ организации. Отличительной особенностью модели O-ISM3 является то, что она основана на оценке зрелости каждого из применяемых в СУИБ процессов управления информационной безопасностью.

Уровни зрелости в O-ISM3 – специальные комбинации процессов, применяющихся при определенных уровнях возможностей. Уровень зрелости определяется как совокупность процессов и возможности каждого из процессов.

Согласно O-ISM3, СУИБ внедряется в рамках четырёх уровней управления информационной безопасностью организации, по которым производится оценка зрелости:

– базовый – для общего управления;

– стратегический (руководство и обеспечение), на котором устанавливаются стратегические цели, осуществляется координация деятельности и обеспечение ресурсами;

– тактический (внесение и оптимизация), который связан с разработкой и реализацией СУИБ, установкой специфических целей и управлением ресурсами;

– операционный (исполнение и отчетность), который связан с достижением определенных целей посредством функционирования технических процессов.

Для каждого из этих уровней в модели определены процессы, которые их обслуживают.

O-ISM3 определяет следующие виды метрик:

– деятельность (Activity) – количество произведенных выходов, их средний срок жизни, среднее время между представлением выходов, среднее время на производство выхода после входа, худшее время на производство выхода после входа;

– область действия (Scope) – доля всех входов, используемых процессом, и доля всех выбранных или тестируемых входов;

– недоступность (Unavailability) – время, прошедшее с момента ожидаемого выполнения процесса после его запуска (время работы), частота и продолжительность перерывов;

– результативность (Effectiveness) – количество входов, среднее время между входами и процент входов, породивших выход;

– эффективность (Efficiency) – отношение числа произведенных выходов к реально доступным для процесса ресурсам;

– загрузка (Load) - процент реально используемых ресурсов;

– качество (Quality) – правильность, точность или другие измерения соответствия выхода начальным целям, если это применимо.

– В O-ISM3 процессы системы управления классифицируются по пяти уровням зрелости: 1 – начальный (Initial); 2 – управляемый (Managed); 3 – определенный(Defined); 4 – контролируемый (Controlled); 5 - оптимизированный (Optimized).

5. Результаты и анализ

Критерии, которые были определены для оценки моделей, рассмотрены ранее в Разделе 3. Результаты анализа моделей зрелости информационной безопасности можно обобщить (таблица 6). В таблице показано соответствие указанным критериям каждой из моделей (C2M2, NICE, CCSMM, SSE-CMM, O-ISM3), рассмотренных в предыдущем разделе.

Таблица 6

Сравнительный анализ моделей

Критерии	C2M2	NICE	SSE-CMM	O-ISM3
Ориентированность на информационную безопасность	ДА	ДА	НЕТ	ДА
Применимость к СУИБ	ДА	НЕТ	НЕТ	ДА
Год последнего пересмотра	2014	2014	2014	2017
Полнота применения	ДА	НЕТ	ДА	ДА
Глубина	УГЛУБЛЕННАЯ	ОБЩАЯ	УГЛУБЛЕННАЯ	УГЛУБЛЕННАЯ
Уровень документации для реализации	СРЕДНЯЯ	СРЕДНЯЯ	ВЫСОКАЯ	ВЫСОКАЯ

По результатам анализа можно сделать вывод, что более конкретные модели предоставляют больше информации для надлежащей классификации и оценки их практики, а также предоставляют более подробные руководящие принципы для повышения уровня показателей зрелости.

ЗАКЛЮЧЕНИЕ

На сегодняшний день анализ и оценка зрелости ИБ является гарантией обеспечения эффективности бизнес-процессов организации. Выбор подходящей модели позволяет оптимизировать процесс управления информационной безопасностью.

Все рассмотренные модели могут быть адаптированы к использованию для оценки зрелости информационной безопасности. Тем не менее, они нуждаются в некотором уровне доработки применительно к конкретной организации. Основные результаты, полученные в результате сравнении, следующие:

– Более общая модель (NICE), не охватывает все области организации, не применима к СУИБ.

– SSE-CMM хоть и адаптирована к использованию на информационную безопасность, не имеет необходимой возможности для применения для оценки зрелости СУИБ

– Единственные модели зрелости, которые применимы к СУИБ, обновлены и ориентированы на всю организацию, - это C2M2 и O-ISM3.

ЛИТЕРАТУРА

[1]. Select Business Solutions. [Electronic resource]. Accecc: http://www.selectbs.com/ process-maturity/ what-is-the-capability-maturity-model.

[2]. M. Lessing: Best practices show the way to Information Security Maturity. [Electronic resource]. Accecc: http:// researchspace. csir. co. za/ dspace/ bitstream/handle/10204/3156/Lessing6_2008.pdf?sequence=1&isAllowed=y.

[3]. G. White, "The community cyber security maturity model". *In: IEEE International Conference on Technologies for Homeland Security*, pp. 173-178, 2011.

[4]. SSE-CMM. [Electronic resource]. Accecc: https://pqm-online.com/assets/files/lib/std/gost_r_iso_mek_21827-2010.pdf.

[5]. *Department of Energy: Cybersecurity Capability Maturity Model (C2M2): Version 1.1*, Department of Homeland Security, 2014.

[6]. *US Department of Homeland Security.: Cybersecurity Capability Maturity Model: Version1.0.* White paper, Department of Homeland Security, 2014. [Electronic resource]. Accecc: https://niccs.us-cert.gov/sites/default/ files/ Capability%20 Maturity% 20Model% 20White%20Paper.pdf?trackDocs=Capability%20Maturity%20Model%20White%20Paper.pdf.

[7]. The Open Group.: Open Information Security Management Maturity Model (O-ISM3). Technical report, Open Group, 2017.

[8]. Н. Милославская, Р. Сагиров, *Обзор моделей зрелости процессов управления информационной безопасностью.*

COMPARATIVE ANALYSIS OFMATURITY MODELS TO EVALUATE INFORMATION SECURITY

Information security can be defined as: the protection of information assets by processing risks of violating the confidentiality, integrity and availability of information that is processed, stored and transmitted between interconnected information systems; and a process that includes preventing, detecting and responding to information security threats. In world practice, the concept of maturity model is used to determine the stage of organizational and technological development of an organization and its processes. To measure the state of the process, a set of metrics is used that represent certain characteristics. Evaluation of these metrics according to the established scale shows the state of the processes, which will characterize the level of their maturity. In world practice, in contrast to Ukrainian practice, the application of the maturity model for managing information security processes is widespread. An example of this is the ISO27000 series of standards that governs information security management issues implemented on the basis of the Information Security Management System. Obviously, before an organization engaged in information security management, sooner or later the question arises of how to fulfill these requirements, to what extent and at what level of detail, etc. Maturity model can help to answer these and other questions, on the basis of which the level of maturity of information security processes will be evaluated. To identify the main models of information security maturity, an analysis of open sources and best practices related to information security maturity models was carried out. Based on the results of the analysis of the sources, the most applicable models of information security maturity were determined, namely: SSE-CMM, C2M2, NICE and O-ISM3.

Keywords: information security; maturity model; ISO 27001; ISMS; comparative analysis; metrics.

ПОРІВНЯЛЬНИЙ АНАЛІЗ МОДЕЛЕЙ ОЦІНКИ ЗРІЛОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Інформаційна безпека може бути визначена як: захист інформаційних активів за допомогою обробки ризиків, спрямованих на порушення конфіденційності, цілісності та доступності інформації, яка обробляється, зберігається і передається між взаємопов'язаними інформаційними системами; процес, який включає запобігання, виявлення і реакцію на загрози інформаційній безпеці. Мета даної статті - описати і порівняти найбільш використовувані моделі зрілості інформаційної безпеки для аналізу їх відповідності цілям використання спільно з стандартом ISO 27001. У статті показано, що моделі зрілості інформаційної безпеки мають схожі елементи, домени і рівні зрілості. Вони також грунтуються на оцінці ризиків, хоча і на різних рівнях глибини. Було відзначено, що кожна модель в силу своєї специфіки має різні сфери застосування. У світовій практиці для визначення стадії організаційного і технологічного розвитку організації і її процесів застосовується поняття моделі зрілості. Для вимірювання стану процесу використовується набір метрик, які представляють собою певні характеристики. Оцінювання цих метрик за встановленою шкалою показує стан процесів, яке і буде характеризувати рівень їх зрілості. У світовій практиці, на відміну від української, застосування моделі зрілості для управління процесами інформаційної безпеки широко поширене. Прикладом цього може служити серія стандартів ISO27000, яка регулює питання управління інформаційною безпекою, що реалізуються на основі Системи Управління Інформаційною Безпекою. Очевидно, що перед організацією, що здійснює діяльність з управління інформаційною безпекою, рано чи пізно постає питання про те, як виконувати ці вимоги, в якому обсязі і на якому рівні деталізації і т.п. Відповісти на ці та інші питання може допомогти модель зрілості, на основі якої буде проводиться оцінка рівня зрілості процесів інформаційної безпеки. Для визначення основних моделей зрілості інформаційної безпеки було проведено аналіз відкритих джерел і кращих практик, пов'язаних з моделями зрілості інформаційної безпеки. На підставі результатів аналізу джерел були визначені найбільш прийнятні моделі зрілості інформаційної безпеки, а саме: SSE-CMM, C2M2, NICE і O-ISM3.

Ключові слова: інформаційна безпека; модель зрілості; ISO 27001; СУІБ; порівняльний аналіз; метрики.

Коломицев Михайло Володимирович, кандидат технічних наук, доцент Фізико-технічного інституту НТУУ «КПІ».
E-mail: box144.85@gmail.com.
Orcid ID: 0000-0001-8460-3041.
Коломыцев Михаил Владимирович, кандидат технических наук, доцент Физико-технического института НТУУ «КПИ».
Kolomytsev Myhailo, candidate of technical sciences, associate professor of Institute of Physics and Technologies of the NTUU "KPI".

Носок Світлана Олександрівна, кандидат технічних наук, доцент Фізико-технічного інституту НТУУ «КПІ».
E-mail: nos.sv.ol@gmail.com.
Orcid ID: 0000-0002-0016-9346
Носок Светлана Александровна, кандидат технических наук, доцент Физико-технического института НТУУ «КПИ».
Nosok Svitlana, candidate of technical sciences, associate professor of Institute of Physics and Technologies of the NTUU "KPI".

Тоцький Роман Олександрович, студент Фізико-технічного інституту НТУУ «КПІ».
E-mail: r.totskyi@gmail.com.
Orcid ID: 0000-0001-9695-0681.
Тоцкий Роман Александрович, студент Физико-технического института НТУУ «КПИ».
Totskyi Roman, student of the Institute of Physics and Technologies of the NTUU "KPI".