

ПРИМЕНЕНИЕ МОДЕЛИ ЗРЕЛОСТИ ДЛЯ ОЦЕНКИ КОМПЛЕКСА МЕР ПО ПРОТИВОДЕЙСТВИЮ ВНУТРЕННИМ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Поляничко Марк Александрович

кандидат технических наук, доцент,

Петербургский государственный университет

пути сообщения Императора Александра I, г. Санкт-Петербург

Аннотация. Модели зрелости возможностей (СММІ) используются для поэтапного совершенствования различных процессов в организациях. Приведенные характеристики уровней зрелости позволяют классифицировать возможности организации по выявлению внутренних угроз информационной безопасности и противостоянию им.

Ключевые слова: внутренние угрозы информационной безопасности, инсайдер, СММІ, модель зрелости, управление информационной безопасностью

Внутренние (инсайдерские угрозы) информационной безопасности — это угрозы, исходящие от работников организации [7]. Зависимость современных организаций от используемых информационных технологий и информационных активов свидетельствует о том, что проблема инсайдеров будет приобретать всё большую актуальность [2]. Обнаружение инсайдеров может осуществляться путем внедрения комплекса организационных и технологических мер [1,5].

Для оценки внедренного комплекса мер предлагается использовать модель зрелости процессов. Capability Maturity Model Integration (СММІ) – набор моделей (методологий) совершенствования рабочих процессов в организациях. СММІ содержит набор рекомендаций в виде практик, внедрение которых позволяет достичь цели, необходимые для полноценного функционирования определённых областей деятельности [4]. Любое совершенствование процессов подразумевает плавный/поэтапный процесс. В СММІ эти этапы формализованы – существует 5 уровней зрелости (Таблица 1), каждый из которых указывает на зрелость процессов организации.

Таблица 1 – Уровни зрелости управления

Название уровня	Описание
1. Начальный	Процессы не определены либо непредсказуемые и неконтролируемые.
2. Интуитивно управляемый	Определены единичные процессы. Зачастую процессы появляются в ответ на определенные события.

3. Определенный	Процессы определены на уровне всей организации. Процессы выполняются заблаговременно.
4. Управляемый количественно	Процессы измеряются и контролируются.
5. Оптимизируемый	Процессы непрерывно совершенствуются.

В данной статье предлагаются характеристики уровней модели СММІ применительно к процессам управления противодействием внутренним угрозам. Предлагаемые уровни приведены ниже.

Начальный уровень зрелости управления процессами противодействия инсайдерской угрозе

Характеристика уровня:

- Существуют отдельные изолированные процессы или функции.
- Отсутствуют четко определенные роли и обязанности.
- В основном реактивная деятельность с минимальной или вообще без официальной стратегии профилактики.

Результирующее состояние:

- Повышенный уровень проявления инсайдерской угрозы.
- Медленная реакция в случае, если угроза будет реализована.

Интуитивно управляемый уровень зрелости управления процессами противодействия инсайдерской угрозе

Характеристика уровня:

- Используются существующие процессы или функции безопасности для предотвращения инсайдерской угрозы, формальная программа противодействия инсайдерской угрозе отсутствует.
- Отсутствует формализованное обучение для сотрудников или поставщиков.
- Связность процедур неразвита.

Результирующее состояние:

- Ограниченные возможности обнаружения.
- Непоследовательность в реагировании, в зависимости от характера инцидента.
- Неадекватные процедуры управления последствиями.

Определенный уровень зрелости управления процессами противодействия инсайдерской угрозе

Характеристика уровня:

- Существует формальная программа противодействия инсайдерской угрозе со специализированными политиками и процессами, которые согласуются с существующими программами информационной и корпоративной безопасности.
- Принята стратегия обнаружения инсайдерских угроз.
- Созданы планы реагирования на инциденты, включающие обработку событий внутренних угроз.
- Введены официальные процедуры управления последствиями.
- Созданы информационные ресурсы, посвященные инсайдерской угрозе.
- Разработана учебная программа для сотрудников и поставщиков.
- Отсутствует полное понимание важнейших активов организации.

Результирующее состояние:

- Общеорганизационная осведомленность об инсайдерских угрозах.
- Повышенная способность обнаруживать инсайдерские угрозы с помощью традиционных технологий информационной безопасности, таких как защита от потери данных, мониторинг конечных точек и т. д.
- Оперативная эффективность, достигнутая благодаря скоординированным усилиям всех заинтересованных сторон.
- Согласованность мониторинга и защиты активов.
- Единообразие в обработке инцидентов .
- Некоторые критически важные активы более подвержены инсайдерским угрозам, чем другие.

Управляемый количественно уровень зрелости управления процессами противодействия инсайдерской угрозе

Характеристика уровня:

- Созданы ключевые показатели эффективности для оценки эффективности программы.
- Внедрен итеративный подход, обеспечивающий непрерывное улучшение.
- Сильная дисциплина управления информацией, лежащей в основе программы противодействия инсайдерским угрозам.
- Существуют отдельные индикаторы риска, разработанные для мониторинга критических активов.
- Использует технологии анализа данных, такие как поведенческий анализ, для выявления скрытых связей и мотивов.

Результирующее состояние:

- Всестороннее понимание важнейших активов организации и связанных с ними рисков [3].

- Расширенные возможности мониторинга и устранения внутренних угроз.
- Постоянное совершенствование программы.
- Захватывает ранее пропущенные признаки, указывавшие на наличие потенциальной инсайдерской угрозы.
- Измеримое снижение числа инцидентов с инсайдерской угрозой.

Оптимизируемый уровень зрелости управления процессами противодействия инсайдерской угрозе

Характеристика уровня:

- Программа противодействия инсайдерским угрозам полностью интегрирована в стратегию управления рисками предприятия.
- Упреждающей защите и реагированию на инсайдерские угрозы уделено повышенное внимание.
- Развернута инфраструктура Big Data, обеспечивающая доступ и интеграцию всех необходимых источников данных в организации.
- Расширенный набор индикаторов риска с использованием платформы больших данных, передовых технологий анализа данных и организационных знаний.

Результатирующее состояние:

- Значительное снижение случаев реализации инсайдерской угрозы.
- Расширяет преимущества программы противодействия инсайдерским угрозам на другие бизнес-императивы, такие как управление рисками, внутренний контроль и управление талантами.
- Повышение защищенности процессов внутреннего контроля и потенциала управления рисками организации.
- Своевременное реагирование на судебные и нормативные запросы о предоставлении данных.

Заключение

Модели зрелости эффективно применяются в качестве инструмента объективной оценки степени повторяемости, последовательности и эффективности определенных видов деятельности или процессов в различных областях деятельности [4]. Инсайдерская угроза не является новым риском, но применение человеко-ориентированного подхода при обеспечении информационной безопасности является достаточно новой практикой [6, 7]. Приведенные характеристики уровней зрелости позволяют классифицировать возможности организации по выявлению внутренних угроз информационной безопасности и противостоянию им.

Список литературы:

1. Chinchani R. [и др.]. Towards a theory of insider threat assessment // International Conference In Dependable Systems and Networks. 2005. С. 108–117.
2. Insider Threat Report: 2018 - CA Technologies // CA Technologies URL: <https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf> (дата обращения: 18.07.2018).
3. McCurry J. [и др.]. A holistic approach to dealing with risk from within // Managing insider threat. 2016. С. 1–16.
4. Денис М. Ахен, Арон Клауз, Ричард Тернер CMMI: Комплексный подход к совершенствованию процессов. Практическое введение в модель. — М: «МФК», 2005, 300 с. ISBN 5-85389-082-4.
5. Поляничко М.А. Внутренние угрозы информационным системам на транспорте // Интеллектуальные системы на транспорте Сборник материалов Первой международной научно- практической конференции. - СПб.: Петербургский государственный университет путей сообщения Императора Александра I. (2011).
6. Поляничко М.А., Пунанова К.В. Проблемы применения человеко-ориентированного подхода к обеспечению кибербезопасности // Научно-практические исследования. 2018. № 13 (4). С. 107–110.
7. Поляничко М.А., Пунанова К.В. Основные проблемы практического применения человеко-ориентированного подхода к обеспечению информационной безопасности // «Фундаментальные и прикладные разработки в области технических и физико-математических наук» Сборник научных статей по итогам работы третьего международного круглого стола. - М.: Общество с ограниченной ответственностью «КОНВЕРТ». 2018. С. 57–60.