Таким чином, аналіз можливості застосування гіперграфів, як інструменту моделювання в задачах інформаційної безпеки дозволяє зробити висновок, що використання зазначеного інструментарію є достатньо перспективним для вирішення задач синтезу та аналізу моделі загроз автоматизованій системі обробки інформації класу 3 та оцінки рівня її захищеності.

Список літератури

1. Многоуровневая декомпозиция гиперграфовых структур (Електрон. ресурс.) / Спосіб доступу: URL: http://wwwcdl.bmstu.ru/it/batischev1.html – Загол. з екрана.

2. Емеличев В.А., О. И. Мельников, В. И. Сарванов, Р. И. Тышкевич Глава XI: Гиперграфы // Лекции по теории графов. – М.: Наука, 1990. – С. 298– 315. – 384 с.

3. Омельченко Г.Г. Гиперграфовые модели и методы решения дискретных задач управления в условиях неопределенности.

4. Омельченко Г.Г. Гиперграфовые модели и методы решения дискретных задач управления в условиях неопределенности, диссертация на соискание ученой степени кандидата физико-математических наук, 2004.

5. Зыков А.А. Гиперграфы // Успехи математических наук. – 1974. – № 6 (180).

МЕТРИКИ ЭФФЕКТИВНОСТИ ПРОЦЕССОВ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Д.С. Тимофеев, И.А. Ковальская
(Украина, Днепропетровск, ГВУЗ «Национальный горный университет»)

В процессе управления любым направлением деятельности необходимо вырабатывать осознанные и эффективные решения, принятие которых помогает достичь определенных целей. Решение можно принять только на основании фактов и анализа причинно-следственных связей.

Метрика - это инструмент, позволяющий взвешенно и объективно принимать управленческие решения по улучшению работы мер и процессов по обеспечению информационной безопасности (ИБ). Отслеживая метрики на регулярной основе, можно выявить недостатки (или потенциальные недостатки) в процессах обеспечения ИБ и принять своевременные и обоснованные меры по их улучшению и устранению коренных причин возникших отклонений.

Метрики необходимы для того, чтобы:

- показать, каким образом деятельность по безопасности вносит непосредственный вклад в достижение целей безопасности;
- измерить, как изменения в процессе отражаются на достижении целей безопасности;
- выявить существенные аномалии в процессах и принять обоснованные решения по исправлению или улучшению процессов [3].

Для создания эффективных критериев оценки системы управления информационной безопасности используется методика S.M.A.R.T. Согласно данной методике, метрика должна быть:

- конкретной (Specific), ясной и иметь непосредственное отношение к измеряемому процессу;
- измеримой (Measurable), т.е. должна существовать возможность однозначно количественно измерить ее;
- практически применимой (Actionable), т.е. должна существовать возможность воздействия на процесс для улучшения метрики;
- значимой (Relevant): улучшение метрики должно означать повышение вклада процесса в достижение целей безопасности;
- своевременной (timely): для эффективного использования, метрику должно быть возможно достаточно быстро измерить [3].

Необходимо, чтобы периодичность оценки метрик и усилия, прикладываемые к их вычислению, были сопоставимы. Также следует избегать качественных значений для метрик, необходимо стремиться к их количественному выражению. Качественные значения могут использоваться для наглядности, но они всегда должны быть только лишь дополнением к количественным оценкам и не заменять их.

Метрики полностью определяются следующими атрибутами:

- название метрики;
- описание, что измеряется;
- как проводится измерение метрики;
- как часто выполняется это измерение;
- как рассчитываются пороговые значения;
- диапазон значений, считающихся нормальными для метрики;
- наилучшие возможные значения метрики;
- единицы измерения.

Для основных процессов и мер должны быть определены несколько метрик, которые смогут вовремя сигнализировать об отклонениях или потенциальных отклонениях.

Используя метрики для результатов, появляется возможность:

- определить, как изменения в процессе отразились на его результатах;
- выявить существенные аномалии в процессах;
- обосновать решения по исправлению или улучшению процесса [1].

Существует шесть этапов использования метрик: измерение, интерпретация, исследование, представление и диагностирование.

В зависимости от выбранной для оценки ИБ метрики/группы метрик можно разделить способы оценки ИБ организации на оценку по эталону, риск-ориентированную оценку и оценку по экономическим показателям.

Способ оценки ИБ по эталону сводится к сравнению деятельности и мер по обеспечению ИБ организации с требованиями, закрепленными в эталоне. По сути дела проводится оценка соответствия СУИБ организации установленному эталону. Под оценкой соответствия используются, например, показатели ИБ организации установленным метрикам понимается деятельность, связанная с прямым или косвенным определением выполнения или невыполнения соответствующих требований ИБ в организации. С помощью оценки

соответствия ИБ измеряется правильность реализации процессов системы обеспечения ИБ организации и идентифицируются недостатки реализации.

В результате проведения оценки ИБ должна быть сформирована оценка степени соответствия СУИБ эталону, в качестве которого могут быть приняты (в совокупности и отдельно):

- требования законодательства Украины в сфере ИБ;
- отраслевые требования по обеспечению ИБ;
- требования нормативных, методических и организационно распорядительных документов по обеспечению ИБ;
- требования национальных и международных стандартов в области ИБ.

Основные этапы оценки информационной безопасности по эталону включают выбор эталона и формирование на его основе критериев оценки ИБ, сбор свидетельств оценки и измерение критических элементов (факторов) объекта оценки, формирование оценки ИБ.

Риск-ориентированная оценка ИБ организации представляет собой способ оценки, при котором рассматриваются риски ИБ, возникающие в информационной сфере организации, и сопоставляются существующие риски ИБ и принимаемые меры по их обработке. В результате должна быть сформирована оценка способности организации эффективно управлять рисками ИБ для достижения своих целей.

Основные этапы риск-ориентированной оценки информационной безопасности включают идентификацию рисков ИБ, определение адекватных процессов менеджмента рисков и ключевых индикаторов рисков ИБ, формирование на их основе метрик оценки ИБ, сбор свидетельств оценки и измерение риск-факторов, формирование оценки ИБ [2].

Способ оценки ИБ на основе экономических показателей оперирует понятными для бизнеса аргументами о необходимости обеспечения и совершенствования ИБ. Для проведения оценки в качестве метрик эффективности СУИБ совокупной стоимости владения (Total Cost of Ownership — TCO).

Список литературы

1.Информационная безопасность для организаций с высоким уровнем риска: новые угрозы и возможные подходы к их нейтрализации [Электронный ресурс]. – Режим доступа: http://www.jetinfo.ru/stati/organizatsionye-i-pravovye-aspekty-informatsionnoj-bezopasnosti/informatsionnaya-bezopasnost-dlya-organizatsij-s-vysokim-urovnem-riska-novye-ugrozy-i-vozmozhnye-podkhody-k-ikh-nejtralizatsii/2007

2.Способы оценки информационной безопасности [Электронный ресурс]. – Режим доступа: http://www.cfin.ru/appraisal/business/special/infosec.shtml

3.Метрики безопасности [Электронный ресурс]. – Режим доступа: http://dorlov.blogspot.com/2009/11/blog-post.html