МЕТРИКИ БЕЗОПАСНОСТИ

Денис Салтыков,
Молдавская Экономическая Академия (Республика Молдова)

This article presents general information about security metrics. Also, here will be described common classification and the main goal of security metrics with advice for the best choice of special security metrics.

Цели использования метрик безопасности.

Тема метрик безопасности является современной и актуальной, так как настоящее время можно охарактеризовать как эпоху информации, когда информация является без преувеличения самой важной основной ценностью в обществе. Таким образом, не менее актуальным является вопрос информационной безопасности и защиты информации. Метрики информационной безопасности, правильный подбор нужных метрик и методов их расчета отражают эффективность системы защиты информации и позволяют на их основе улучшать характеристики системы.

Актуальность данной темы подтверждают результаты опроса ISACA – "Critical Elements of Information Security Program Success".. Как вывод были выведены 5 основных критериев успеха:

1. Общий язык. Бизнес первичен.
2. Процесс взаимодействия. Двусторонняя связь.
3. Система убеждения. Маркетинг и PR.
4. Выход на руководство. Сила и влияние.
5. Метрики. Что и как измерять.

Можно задать вопрос: можно ли вообще измерять? Если что-то лучше, значит, есть признаки улучшения. В таком случае улучшение можно наблюдать, наблюдаемое улучшение можно посчитать. То, что можно посчитать, можно измерить, а измеренное – оценить и продемонстрировать. Таким образом, можно сделать вывод, что тема метрик информационной безопасности актуальна, так как явно отображает безопасность на уровне бизнеса, а значит, помогает увеличить экономическую эффективность работы любого предприятия в любой отрасли.

Метрики необходимы для того, чтобы:

* показать, каким образом деятельность вносит непосредственный вклад в достижение целей;
* измерить, как изменения в процессе отражаются на достижении целей;
* выявить существенные ано-

малии в процессах и принять обоснованные решения по исправлению или улучшению процессов.

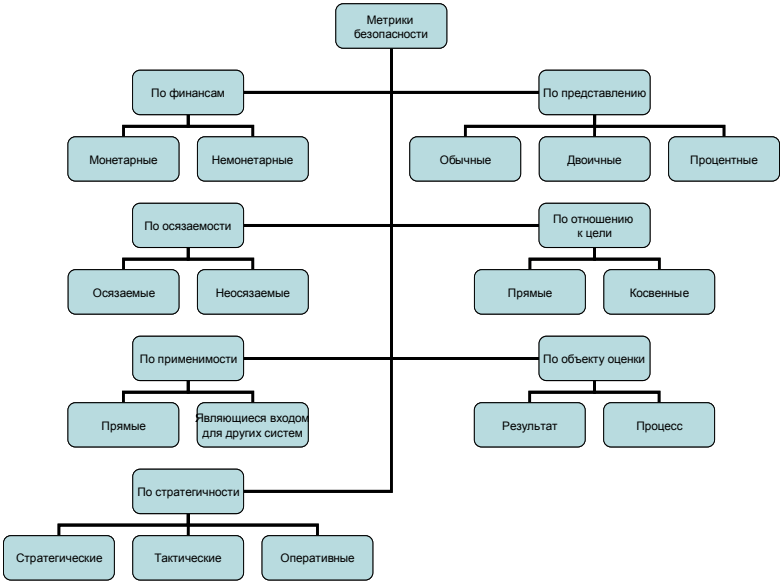
Выбор правильных метрик.

Следует отметить, что стандартного набора метрик безопасности, который подошёл бы на все случаи жизни не существует. Любой объект обладает собственной спецификой, так что в каждом конкретном случае рассчитывается специальный набор метрик, который должен оптимально соответствовать ситуации.

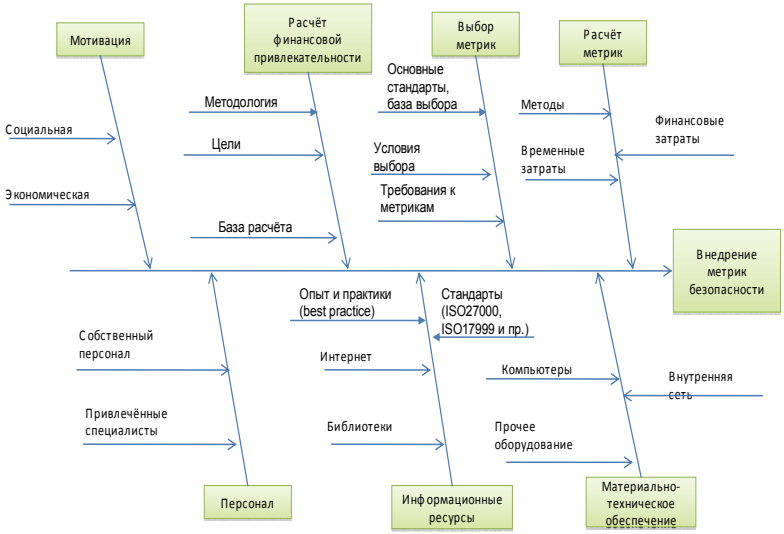
Следует также дать ответ на вопрос, какие метрики подойдут лучше: для целей или для результатов процесса. Отсутствие инцидентов в течение длительного времени приводит к ощущению безопасности, но предотвращённые инциденты не могут быть измерены так же, как реально произошедшие.

Метрики для целей не только трудно найти, они, кроме всего прочего, еще и не очень полезны для управления безопасностью. Это связано с отсутствием прямой связи между деятельностью по безопасности и, собственно, целями безопасности. Вы никогда не сможете сказать, действительно ли Вы приблизились к целям безопасности, оказав определенное воздействие на процессы безопасности.

Классификация метрик безопасности.



Если метрики для целей трудно получить, и они не очень полезны, то измерение результатов процесса обеспечения безопасности не только возможно, но и крайне полезно, так как результаты прямо или косвенно связаны с обеспечением безопасности, уверенности и достоверности.



Литература:

1. Астахов А. Искусство управления информационными рисками, Москва, ДМК Пресс, 2010.
2. Мельников В. П., Клейменов С. А., Петраков А. М.. Информационная безопасность и защита информации, Москва, Издательский центр «Академия», 2008.
3. Блог Алексея Лукацкого. http://lukatsky.blogspot.com/