Методические аспекты оценки информационной безопасности организации по критерию уверенности

УДК 004.621:681.324

Юрий Самохвалов[1], Николай Браиловский[2]

Киевский национальный университет имени Тараса Шевченко,
[1]yu1953@ukr.net, [2]bk1972@ukr.net

В действующей практике можно выделить следующие основные типы метрик информационной безопасности (ИБ): метрики реализации, служащие для измерения степени проведения политики безопасности в жизнь; метрики эффективности, служащие для измерения результативности сервисов безопасности. Эти метрики являются основой наиболее распространенных в настоящее время подходов к оценке защищенности информации: верификационного и риск-ориентированного.

При этом данные подходы обладают общим недостатком: полученные в результате применения методик метрики информационной безопасности недостаточно информативны, так как учитывают лишь объективные аспекты безопасности, совершенно игнорируя субъективные. Поэтому они не позволяют выработать обоснованные суждения о состоянии конфиденциальности, целостности и доступности информации и уровне ИБ организации в целом. В связи с этим возникает необходимость в разработке методического аппарата оценки ИБ организации с учетом объективных и субъективных аспектов безопасности. При этом основная проблема заключается в выборе соответствующего критерия и показателя оценки, а также способа его вычисления, что и определяет ***цель данной работы.***

Одним из основных принципов, которым необходимо руководствоваться при выборе критериев оценки ИБ, является безусловное отражение критерием полезности для организации с точки зрения конфиденциальности, целостности и доступности информации. Исходя из этого в качестве критерия оценки предлагается использовать уверенность в том, что организация реализует принятую политику безопасности. А так как уверенность является выражением убежденности, что система ИБ организации обеспечивает конфиденциальность, целостность и доступность информации, следовательно, в качестве показателя уверенности целесообразно использовать показатель полезности (желательности) как значение обобщенной функции желательности Харрингтона. Это позволяет использовать единую универсальную психофизическую шкалу измерения, которая полностью корреспондируется с законом Вебера-Фехнера о нелинейности шкал измерений субъективных суждений.

Оценка уверенности включает оценку доверия к информационной безопасности организации, качества модели оценки доверия и бекграунда лиц, проводивших такую оценку и оценку знаний относительно угроз.

Доверие к ИБ организации (Dc) основывается на доверии к корректности реализации процессов и защитных мер и доверии к эффективности процессов информационной безопасности.

Доверие к корректности (правильности) процессов и защитных мер сводится к оценке степени их соответствия требованиям эталону, в качестве которого выбран стандарт СТО БР ИББС-1.0-2014. Измерение степени выполнения требований осуществлять с помощью шкалы Харрингтона. Эта оценка отражает степень доверия к правильности реализации процессов и защитных мер обеспечения ИБ организации требованиям этого стандарта.

Доверие к эффективности процессов информационной безопасности базируется на требованиях к составу и модели зрелости процессов информационных технологий. Оценку уровня зрелости процессов ИБ проводиться согласно модели Process Capability Model, которая является мерой оценки полноты, адекватности и эффективности процессов менеджмента ИБ. Уровень зрелости процессов ИБ определяется тем, насколько полно и последовательно менеджмент организации руководствуется принципами ИБ, реализует политики и требования ИБ, использует накопленный опыт и совершенствует системы менеджмента информационной безопасности. Эта модель определяет шесть уровней зрелости с нулевого по пятый. Оценку уровня зрелости процессов ИБ проводиться согласно методологии Information Security Forum.

Качество модели оценки доверия (D_P) зависит от того, в какой мере экспертный метод и процедура его реализации обеспечивает объединение математических моделей и оценочных суждений экспертов с целью получения достоверного результата.

Бекграунд (D_B) отображает степень образованности, интеллектуальный уровень, жизненный и профессиональный опыт лиц, которые проводили оценку доверия к ИБ. Оценка бекграунда и качества модели осуществляется по шкале желательности Харрингтона.

Знания относительно угроз (D_z) можно охарактеризовать полнотой и достоверностью информации (свидетельствами) относительно того, что, во-первых, известные угрозы не имеют каналов влияние на бизнес-процессы или они минимизированы (предпринята защита) и мы знаем способности этой защиты, или же ничтожна вероятность возможных угроз. А во-вторых, что имеются средства, способные прогнозировать или выявлять новые угрозы. Под достоверностью информации понимается ее свойство отражать объективную реальность с необходимой точностью. Для оценки достоверности информации используется схема Кента, которая дает наглядную классификацию информации с точки зрения степени ее достоверности. Тогда зная достоверность имеющейся информации относительно угроз и учитывая полноту свидетельств, по шкале Харрингтона определяется полезность этих знаний как фактора обеспечения уверенности.

И, наконец, степень уверенности, с которой в организации реализована политика безопасности (D_U) определяется значением функции:

$$D_U = \sqrt[4]{D_C \cdot D_P \cdot D_B \cdot D_Z}.$$

Рассмотренный подход к оценке ИБ организации является довольно простым в реализации и может быть использован в качестве пилотажа для разработки соответствующих методик оценки ИБ организаций различных форм собственности.