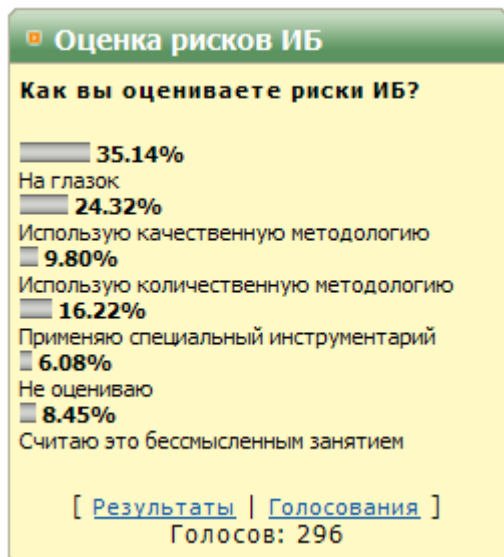


Как оценивают риски наши соотечественники?

написано Александр Астахов | 10 июня, 2023

Среди специалистов нет единодушия в вопросах управления рисками. Нередко можно услышать довольно бессмысленные, как будет показано далее, споры и сопоставления количественных и качественных методов оценки рисков и даже отрицание целесообразности и самой возможности адекватно оценивать риски. Кто-то обвиняет руководство организации в недостаточном осознании важности вопросов безопасности или жалуется на трудности, связанные с получением объективной оценки ценности определенных нематериальных активов, таких, например, как репутация организации. Другие, не видя возможности обосновать расходы на безопасность, предлагают относиться к этому как к некой гигиенической процедуре и тратить на эту процедуру столько денег, сколько не жалко либо сколько осталось в бюджете.

По данным опроса, проводимого на портале ISO27000.ru среди менеджеров информационной безопасности российских компаний, всего 34% менеджеров ИБ пытаются использовать какой-либо систематический подход к оценке рисков, остальные 66% даже не пытаются этого делать, оценивая риски «на глазок» либо вовсе не делая этого. Из них 15%, похоже, даже не понимают существа обсуждаемого вопроса, считая оценку рисков занятием бессмысленным. Еще примерно в 15% организаций для управления информационными рисками используется специализированный программный инструментарий.



Источник: ISO27000.ru

Из
об
ще
ни
я
с
эк
сп
ер
та
ми
,
от
ве
ча
ющ
им
и
за
ин
фо
рм
ац
ио
нн
ую
бе
зо
па
сн
ос
ть
в
ор
га
ни
за

ци
ях
,
мо
жн
о
сд
ел
ат
ь
оп
ре
де
ле
нн
ые
вы
во
ды
от
но
си
те
ль
но
то
го
,
с
ка
ки
ми
тр
уд
но
ст
ям

и
ст
ал
ки
ва
ют
ся
их
по
пы
тк
и
уп
ра
вл
ят
ь
ри
ск
ам
и.
По
от
но
ше
ни
ю
к
да
нн
ом
у
во
пр
ос
у
вс

е
сп
ец
иа
ли
ст
ы
по
др
аз
де
ля
ют
ся
на
че
ты
ре
ха
ра
кт
ер
ны
е
гр
уп
пы
.

Математики

Специалисты, имеющие техническое образование и владеющие определенным математическим аппаратом, склонны задействовать этот аппарат для оценки информационных рисков. Подход, в основе которого лежит стремление получить количественные оценки рисков с использованием математических формул и моделей, быстро заводит в тупик наших коллег, которым пока еще не удалось окончательно забыть школьные и университетские

курсы точных наук и, видимо, в глубине души немного жаль понапрасну проведенное за партой время, затраченное на изучение вещей, которые не удастся приложить к реальной жизни. Углубляясь в математическую статистику, теорию вероятностей, байесовские распределения, теорию нечетких множеств и прочие математические теории, адепты количественного подхода теряют связь с реальной жизнью и бизнес-контекстом, получая ни к чему не приложимые уравнения со множеством неизвестных.

Технари

Технические специалисты, имеющие профильное образование в области ИБ или ИТ, хорошо представляют себе уязвимости, которым подвержены информационные системы и технологии, а также какие меры необходимо предпринимать для их устранения. Однако эти специалисты имеют весьма туманное представление об информационных активах, их ценности и бизнес-процессах организации. Они склонны измерять риск величиной соответствующей уязвимости без учета остальных факторов. Рассуждают эти спецы о рисках на своем птичьем языке, который не доступен для понимания руководству организации и представителям бизнеса. Если технарей попросить оценить риски, то они, скорее всего, представят в качестве отчета о рисках отчет об уязвимостях, полученный при помощи сканера безопасности. Технари идут снизу вверх, концентрируясь на технических деталях реализации тех или иных угроз и совершенно упуская из виду цели бизнеса, для достижения которых необходимо управлять рисками. Им сложно бывает определить, какие угрозы и с какой степенью детализации надо анализировать для принятия решения по рискам.

Аналитики

Аналитики, как правило, владеют подходами и инструментами для управления рисками, но им не хватает практических навыков как в технической сфере, так и в сфере бизнеса. Для адекватной оценки рисков им необходимы как технари с их знанием технологий и сценариев реализации инцидентов, так и представители бизнеса с их знанием бизнес-процессов и

способностью выносить суждения относительно ценности тех или иных активов. Для того чтобы сколотить дееспособную команду из столь разнородных и разнонаправленно мыслящих людей, требуется организационный талант и очень сильная заинтересованность со стороны первых лиц организации.

Скептики

Скептики обычно знают обо всем понемногу и не склонны к глубокому анализу. Они считают оценку рисков задачей неосуществимой, в связи с чем для принятия решений в отношении обеспечения безопасности предпочитают опираться исключительно на собственный опыт, здравый смысл, рекомендации стандартов и нормативных документов. Скептиков, как правило, разочаровывает невозможность точной количественной оценки информационных рисков, а также тот факт, что приходится опираться на субъективные мнения экспертов. К их числу относятся многие руководители служб информационной безопасности, с готовностью рассуждающие о преимуществах системного подхода, однако сами предпочитающие руководствоваться при принятии решений в основном интуицией и устоявшимися представлениями.