Понятие риска

написано Александр Астахов | 10 июня, 2023

Прежде всего необходимо максимально полно и точно определить понятие риска. В BS 7799-3 дается наиболее широкое определение риска как комбинации вероятности события и его последствий. В отличие от спекулятивных рисков, когда событие может носить как позитивный характер (например, выигрыш в казино или на бирже), так и негативный (например, проигрыш), события информационной безопасности всегда носят негативный характер. Это позволяет отнести риски информационной безопасности к категории неспекулятивных рисков.

ISO 27005 конкретизирует понятие информационного риска, раскладывая его на активы, угрозы, уязвимости и ущерб. Согласно ISO 27005: «Риск информационной безопасности – это потенциальная возможность использования уязвимостей актива или группы активов конкретной угрозой для причинения ущерба организации».

Различные определения понятия «информационный риск»:

***Риск** – комбинация вероятности события и его последствий (BS 7799-3:2006).*

***Риск информационной безопасности** – потенциальная возможность использования уязвимостей актива или группы активов конкретной угрозой для причинения ущерба организации (ISO/IEC 27005:2008).*

***Риск** – неопределенность, предполагающая возможность потерь (ущерба) (СТО БР ИББС).*

***Риск** – потенциальная проблема.*

***Риск** – вероятные потери организации в результате инцидентов.*

Понятие риска, данное в ISO 27005, пожалуй, является наиболее полным. Однако можно оперировать и более простыми и легко запоминающимися определениями. Например, риск можно рассматривать просто как потенциальную проблему либо как вероятные потери организации в результате инцидентов. В стандарте Банка России СТО БР ИББС риск определяется как «неопределенность, предполагающая возможность потерь».

Таким образом, риск является комплексной величиной, всегда определяемой через комбинацию ряда других величин. Это обусловливает ошибки в определении и описании конкретных рисков, нередко допускаемые даже специалистами, что вызывает трудности при оценке рисков.

Описание факторов риска, таких как угрозы, инциденты, уязвимости и виды ущерба, по отдельности не является описанием риска. О риске можно говорить только в том случае, если все факторы риска рассматриваются в совокупности. Только комбинация оценочных значений для угроз, уязвимостей и ущерба позволяет получить оценку риска.

Так, вопреки рекламным заявлениям некоторых разработчиков средств защиты информации, сетевые сканеры безопасности, прочие средства анализа защищенности информационных систем, так же как и средства контроля соответствия требованиям, включая средства анализа расхождений (gap analysis), не являются средствами оценки или управления рисками. Такие продукты лишь позволяют выявлять и анализировать определенные категории технических и организационных уязвимостей, а также в ряде случаев идентифицировать определенные классы информационных активов, что, безусловно, является важной частью процесса оценки рисков, который, однако, включает в себя, помимо этого, еще много других элементов.

Чтобы не превращать эту книгу в учебник по основам информационной безопасности, мы вынесли все ключевые

определения, связанные с управлением информационными рисками, в Приложение № 0. Рекомендуется изучить это важное приложение, базирующееся на международных стандартах, обращая внимание на различные факторы и элементы процесса управления риском. Правильное понимание терминологии – существенная часть успеха в овладении мастерством управления рисками.