Глава 4. Оценка рисков информационной безопасности

написано Александр Астахов | 10 июня, 2023

Этапы оценки рисков:

- Анализ рисков:

- Идентификация активов
- Идентификация требований бизнеса и законодательства
- Оценка ценности активов
- Определение приоритетов аварийного восстановления
- Анализ угроз и уязвимостей
- Оценивание рисков:

- Определение величины рисков
- Ранжирование рисков

В этой главе мы переходим к подробному изложению методологии оценки рисков. Согласно устоявшейся терминологии, используемой в стандартах, оценка рисков включает в себя два последовательных этапа: *анализ рисков* и *оценивание рисков*.

Анализ рисков включает в себя:

- идентификацию активов;
- идентификацию бизнес-требований и требований законодательства, применимых к идентифицированным активам;
- оценивание активов с учетом идентифицированных бизнес-

требований и требований законодательства, а также последствий нарушения их конфиденциальности, целостности и доступности;
- идентификацию значимых угроз и уязвимостей идентифицированных активов;
- оценку вероятности реализации угроз и величины уязвимостей.

Оценивание рисков заключается в определении их количественных и качественных значений, формировании реестра рисков и ранжированию рисков.

Далее мы подробно рассмотрим все этапы анализа и оценивания рисков в соответствии с методологией GlobalTrust, базирующейся на международных стандартах и известных методах оценки рисков.