*задание: проанализировать существующие методики оценки рисков ИБ по гос стандартам.*

ГОСТ Р ИСО/МЭК 27005: Данный стандарт предоставляет методику оценки рисков информационной безопасности. Он описывает процесс оценки рисков, начиная от установления контекста и идентификации угроз и уязвимостей, до оценки рисков и принятия решений по управлению ими. ГОСТ Р ИСО/МЭК 27005 предоставляет подходы к оценке вероятности и воздействия угроз, а также методы оценки рисков и принятия решений по управлению ими.

Методика оценки рисков ИБ по этому стандарту включает в себя несколько основных шагов:

1. **Установление контекста**: в этом шаге определяются цели и ограничения оценки рисков, а также контекст, в котором проводится оценка. Важно определить организационную структуру, бизнес-процессы, стейкхолдеров и другие факторы, которые могут повлиять на оценку рисков.

2. **Идентификация активов**: здесь происходит идентификация всех активов организации, которые нужно защищать. Активы могут включать информацию, системы, оборудование, программное обеспечение и другие ресурсы.

3. **Идентификация угроз**: в этом шаге определяются потенциальные угрозы, которые могут нанести вред активам. Угрозы могут быть различными, например, хакерские атаки, физические повреждения или несанкционированный доступ.

4. **Идентификация уязвимостей**: здесь определяются уязвимости активов, то есть слабые места, которые могут быть использованы угрозами для получения несанкционированного доступа или причинения вреда. Это может включать неполадки в системах безопасности, отсутствие обновлений или недостаточную защиту данных.

5. **Оценка вероятности и воздействия угроз**: в этом шаге проводится оценка вероятности возникновения угроз и воздействия этих угроз на активы. Оценка может основываться на исторических данных, экспертных оценках или других методах.

6. **Оценка рисков**: здесь происходит оценка рисков на основе полученных данных об угрозах, уязвимостях, вероятностях и воздействиях. Риски могут быть оценены с помощью различных методов, например, матрицы рисков или качественной шкалы.

7. **Принятие решений по управлению рисками**: после оценки рисков необходимо принять решения по их управлению. Это может включать принятие мер по снижению рисков, переносу рисков или принятию риска с последующим мониторингом.

8. **Документирование и коммуникация результатов**: в этом шаге фиксируются все результаты оценки рисков и принятые решения. Результаты должны быть документированы и представлены заинтересованным сторонам.

9. **Мониторинг и обзор**: после принятия решений по управлению рисками необходимо осуществлять мониторинг и периодический обзор с целью выявления изменений в контексте и эффективности принятых мер по управлению рисками.

Проведение анализа рисков информационной безопасности согласно методике ГОСТ Р ИСО/МЭК 27005 является важным этапом для любой организации, стремящейся обеспечить надежную защиту своей информации и активов. Шаги этой методики позволяют систематически и объективно оценить потенциальные угрозы, уязвимости и риски, с которыми может столкнуться организация.

Путем установления контекста, идентификации активов, угроз и уязвимостей, оценки вероятности и воздействия угроз, а также рисков, организации могут получить полное представление о своей уязвимости перед потенциальными атаками. Принятие решений по управлению рисками на основе результатов анализа помогает снизить вероятность возникновения инцидентов информационной безопасности и минимизировать возможные убытки.

Документирование результатов и регулярный мониторинг обеспечивают постоянное улучшение системы управления рисками информационной безопасности. Такой подход не только помогает предотвратить потенциальные угрозы, но и способствует повышению уровня доверия со стороны клиентов, партнеров и регулирующих органов.

В целом, проведение анализа рисков информационной безопасности в соответствии с ГОСТ Р ИСО/МЭК 27005 является ключевым элементом эффективного управления информационной безопасностью, обеспечивая организации необходимые инструменты для адекватного реагирования на угрозы и защиты своих ценных активов.