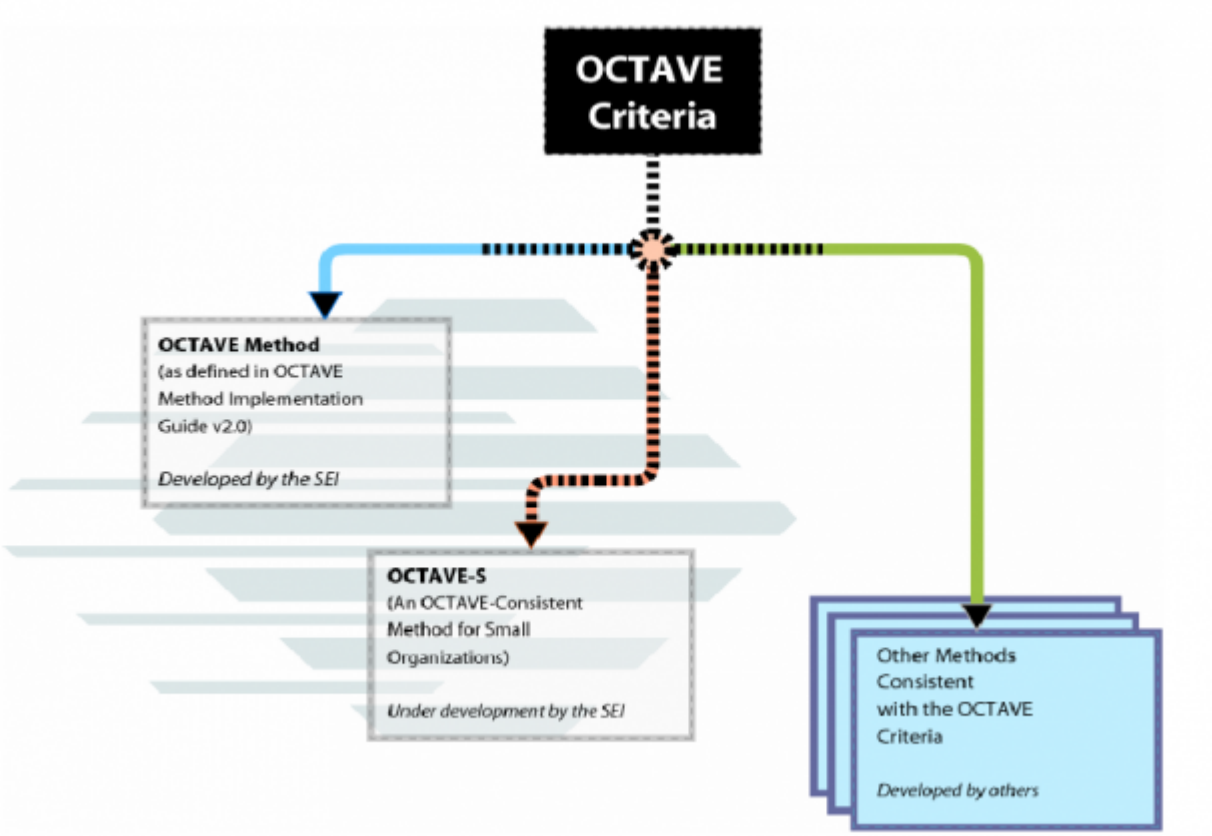
OCTAVE

написано Александр Астахов | 11 июня, 2023
Любой программный продукт, если он действительно является средством для оценки рисков, реализует определенную методологию. Существует достаточное количество хорошо себя зарекомендовавших и широко используемых методов оценки и управления рисками. Некоторые из этих методов повлияли на разработку нашей собственной методологии.

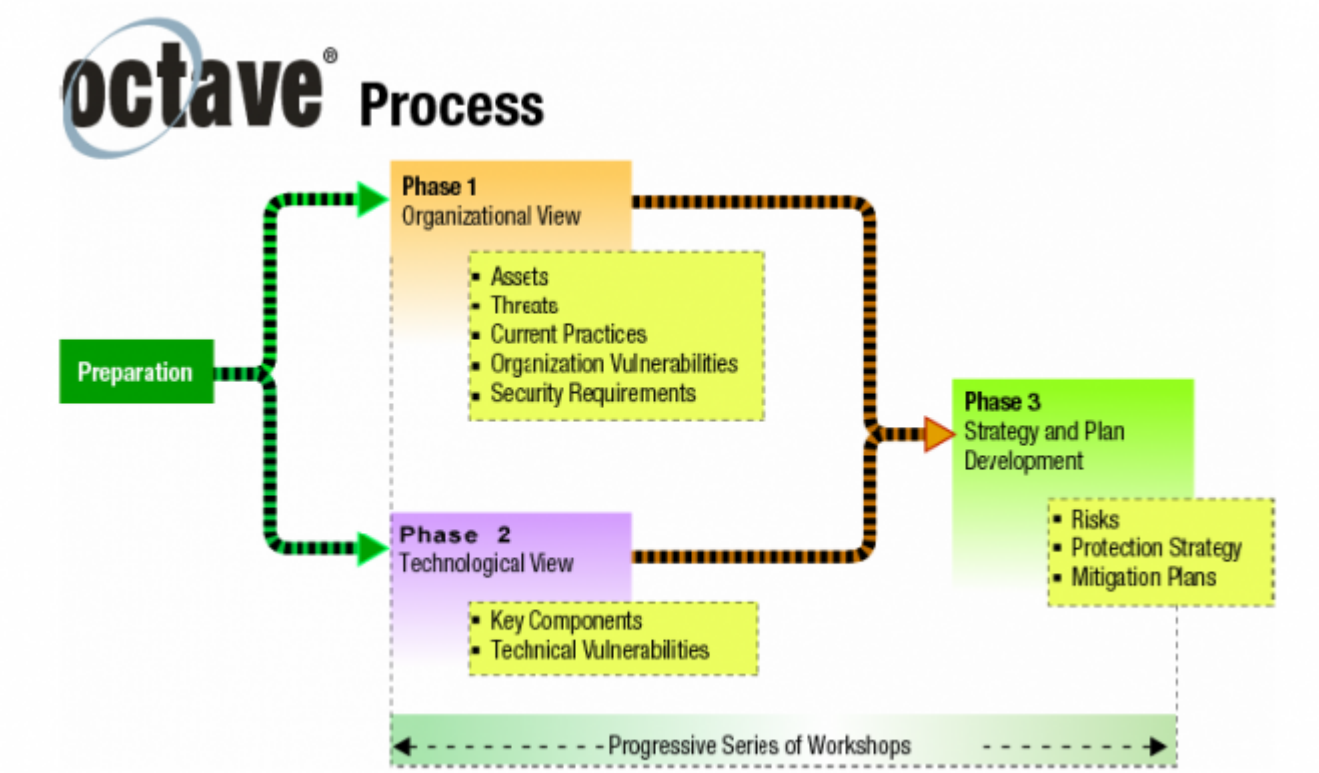
Одним из таких методов является *OCTAVE*, разработанный в университете Карнеги-Мелон для внутреннего применения в организации. OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) – Оценка критичных угроз, активов и уязвимостей – имеет ряд модификаций, рассчитанных на организации различных размеров и областей деятельности. Однако в основе всех модификаций метода OCTAVE лежит набор четко определенных критериев. Эти критерии определяют основные принципы, подходы, процессы, атрибуты и выходные данные оценки рисков, которые мы подробно рассматривать не будем, а вместо этого отошлем читателя к многочисленной литературе, посвященной методу OCTAVE. Исчерпывающую информацию о данном методе оценки рисков на английском языке можно также найти на сайте разработчика по адресу: http://www.cert.org/octave.

В настоящее время представлено три модификации метода OCTAVE:

- Методология оценки рисков OCTAVE Method, подходящая для достаточно крупных организаций (от 300 человек и более)
- Упрощенная методология оценки рисков OCTAVE-S, ориентированная на организации небольшого размера (не более 100 человек)
- Методология оценки рисков OCTAVE Allegro, которая может применяться консультантами на индивидуальной основе, без широкого вовлечения в процесс оценки рисков сотрудников организации



Сущность универсальной методологии OCTAVE Method заключается в том, что для оценки рисков используется последовательность соответствующим образом организованных внутренних семинаров (workshops). Оценка и обработка рисков осуществляется в три этапа, которым предшествует набор подготовительных мероприятий, включающих в себя согласования графика семинаров, назначения ролей, планирование и координацию действий участников рабочей группы по оценке рисков.



На первом этапе, в ходе практических семинаров, осуществляется разработка профилей угроз, включающих в себя инвентаризацию и оценку ценности активов, идентификацию применимых требований законодательства и нормативной базы, идентификацию угроз и оценку их вероятности, а также определение системы организационных мер по поддержанию режима ИБ.

*На втором этапе*производится технический анализ уязвимостей информационных систем организации в отношении угроз, чьи профили были разработаны на предыдущем этапе, который включает в себя идентификацию имеющихся технических уязвимостей и оценку их величины.

*На третьем этапе*производится оценка и обработка рисков ИБ, включающая в себя определение величины и вероятности причинения ущерба в результате осуществления угроз безопасности с использованием уязвимостей, которые были идентифицированы на предыдущих этапах, определение стратегии защиты, а также выбор вариантов и принятие решений по обработке рисков. Величина риска определяется как усредненная величина годовых потерь организации в результате реализации угроз безопасности.

Этапы управления рисками по методу OCTAVE:

1. *Подготовка. Согласования, назначения, планирование, координация.*
2. *Разработка профилей угроз. Активы, требования, организационные меры, угрозы.*
3. *Технический анализ уязвимостей. Анализ защищенности.*
4. *Оценка и обработка рисков. Ущерб, риски, стратегия защиты, план обработки рисков.*

Применение метода OCTAVE, как, впрочем, и любой другой методологии оценки рисков, не требует обязательного использования программного инструментария.