Аудит и оценка рисков

написано GlobalTrust.ru | 20.08.2023

Что представляет собой аудит информационной безопасности?

Аудит информационной безопасности представляет собой комплекс работ, включающий исследование всех аспектов обеспечения информационной безопасности в организации, проводимое по согласованному с заказчиком плану, в соответствии с выбранной методикой и критериями.

При выполнении работ по техническому аудиту и анализу защищенности информационных систем специалисты GlobalTrust используют наиболее продвинутые методы, средства и источники информации, включая Open-Source Security Testing Methodology Manual (OSSTMM), SANS Top Twenty Vulnerabilities List, CVE, CERT Bulletines, SANS SCORE, CIS Security Benchmarks, Nessus и др.

Основным продуктом аудита является Аудиторский отчет, который содержит описание текущего состояния информационной безопасности в организации, описание обнаруженных уязвимостей и несоответствий выбранным критериям аудита, а также рекомендации по их устранению.

Цели аудита

Основными целями проведения работ по аудиту информационной безопасности организации являются:

- Независимая оценка текущего состояния
- Идентификация и ликвидация уязвимостей
- Технико-экономическое обоснование механизмов безопасности
- Обеспечение соответствия требованиям действующего законодательства
- Минимизация ущерба от инцидентов безопасности

Ценность аудита

Ценность аудита информационной безопасности для потенциальных клиентов заключается в следующем:

- Аудит представляет собой независимое исследование, что повышает объективность его результатов (никто не может достаточно эффективно контролировать и оценивать самого себя)
- Эксперты по безопасности, проводящие аудит, имеют более высокую квалификацию и больший опыт подобной работы, нежели штатные сотрудники организации
- Дешевле поручить выполнение этих работ сторонней, специализирующейся на аудите безопасности, организации, чем организовать эти работы у себя
- Наличие официальных сертификатов, аттестатов и аудиторских заключений, выданных авторитетной и уполномоченной на это государством организацией повышает степень доверия к компании со стороны клиентов, партнеров и государственных органов, т.к. это в определенной степени гарантирует адекватную защищенности информационных ресурсов компании.
- Аудит информационной безопасности предшествует работам по созданию системы защиты информации, либо ее модернизации.

Методика, процедура и критерии аудита

Процедура аудита

- Инициирование и планирование
- Обследование, документирование и сбор информации
- Анализ полученных данных и уязвимостей
- Выработка рекомендаций
- Подготовка отчетных документов и сдача работ

Критерии аудита

- Международные, национальные и отраслевые стандарты
- Законодательная и нормативная база
- Внутренние организационно-распорядительные документы организации
- Требования, сформулированные по результатам оценки рисков

Методика аудита

- Методы анализа защищенности, включая тесты на проникновение (penetration testing), анализ конфигурации средств защиты информации, анализ сценариев осуществления атак и использование списков проверки (checklists)
- Интервью с сотрудниками организации с использованием заранее подготовленных и стандартизованных опросных листов
- Документирование системы и анализ рисков с использованием специализированного программного инструментария и шаблонов отчетов
- Анализ организационно-распорядительной документации по обеспечению режима информационной безопасности
- Оценка процессов обеспечения информационной безопасности в организации, квалификации сотрудников, знания ими своих должностных обязанностей и степени их осведомленности в вопросах информационной безопасности
- Оценка достаточности физических механизмов безопасности

Что представляет собой оценка риска?

Оценка рисков включает в себя мероприятия по определению того какие ресурсы и от каких угроз надо защищать, а также в какой степени те или иные ресурсы нуждаются в защите. Риск определяется вероятностью причинения ущерба и величиной ущерба, наносимого организации, в случае осуществления угрозы безопасности. Оценка рисков состоит в том, чтобы выявить существующие риски и оценить их величину.

Процедура оценки риска

Процедура оценки рисков включает в себя ряд последовательных этапов:

- Настойка методологии оценки под конкретную организацию
- Выбор шкалы оценки рисков
- Оценка стоимости ресурсов, вероятности угроз и величины уязвимостей
- Определение допустимого уровня остаточных рисков
- Оценивание рисков
- Подготовка отчета по результатам оценки рисков
- Разработка реестра информационных рисков
- Принятие решений по обработке рисков
- Разработка Плана обработки рисков
- Разработка Декларации о применимости
- Согласование и презентация отчетных документов

Методика оценки риска

При выполнении работ по оценке информационных рисков и внедрению процессов управления рисками в организации специалисты GlobalTrust используют широко распространенную во всем мире методологию OCTAVE, разработанную в университете Карнеги-Мелон (США), а также международный стандарт ISO/IEC 27005.

OCTAVE – Оценка критичных угроз, активов и уязвимостей (Operationally Critical Threat, Asset, and Vulnerability Evaluation) имеет ряд модификаций, рассчитанных на организации разного размера и области деятельности. Сущность этого метода заключается в том, что для оценки рисков используется последовательность соответствующим образом организованных внутренних семинаров (workshops). Оценка рисков осуществляется в три этапа, которым предшествует набор подготовительных мероприятий, включающих в себя согласования графика семинаров, назначения ролей, планирование, координация действий участников проектной группы.

Этапность оценки риска

На первом этапе, в ходе практических семинаров, осуществляется разработка профилей угроз, включающих в себя инвентаризацию и оценку ценности активов, идентификация 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 уязвимостей информационных систем организации 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.

Как часто следует проводить аудит и оценку рисков?

Аудит информационной безопасности и оценка рисков являются обязательными механизмами контроля для любой организации. Они должны проводиться не реже одного раза в год независимыми экспертами, имеющими соответствующую квалификацию и опыт. Это позволяет руководству организации, ее акционерами и третьим сторонам получить объективную информацию о состоянии ее информационной безопасности.

Заказ услуг

- по телефону: +7 (925) 203-95-11
- по e-mail: info@globaltrust.ru
- через web-форму