

Техническое проектирование систем защиты информации

написано GlobalTrust.ru | 27.08.2023

Цели и задачи разработки технического проекта системы защиты информации

Техническое проектирование является необходимым условием для реализации комплексного подхода к созданию систем обеспечения информационной безопасности и защиты информации. В отсутствие технического проекта возможно лишь реализация фрагментарных мер и механизмов безопасности, за счет которых в современных условиях невозможно решение основных вопросов обеспечения информационной безопасности.

Целью проектирования системы защиты информации является выработка рекомендаций, организационных и технических решений по обеспечению безопасности информационных ресурсов хранимых, обрабатываемых и передаваемых по каналам связи в компьютерных сетях и информационных системах организации.

Разработка технического проекта, осуществляется на основе согласованного с заказчиком Технического задания и существующей Концепции обеспечения информационной безопасности.

Специалисты GlobalTrust в ходе технического проектирования проанализируют существующие цели и задачи информационной безопасности, оценят возможное влияние механизмов безопасности на бизнес процессы организации, произведут обоснованный выбор средств и механизмов защиты информации и документируют технические решения по составу средств защиты и способам их взаимодействия.

Архитектура системы защиты информации

Система защиты информации представляет собой совокупность мер организационного и программно-технического уровня, направленных на защиту информационных ресурсов организации от угроз безопасности. Экономический эффект от внедрения системы защиты информации проявляется в снижении величины возможного материального, морального и иных видов ущерба, наносимого организации, за счет мер, направленных на формирование и поддержание режима ИБ.

Система защиты информации в современных организациях имеет сложную многокомпонентную, многоуровневую, территориально и логически распределенную архитектуру. Компоненты системы защиты информации очень тесно интегрированы в информационную инфраструктуру организации. Помимо программных и технических средств обеспечения ИБ, которые могут быть встроены в телекоммуникационное и компьютерное оборудование, операционные системы и приложения, а также специализированных (наложенных) средств защиты информации, архитектура системы включает в себя также систему организационных мероприятий и ИТ-процессов. Для построения системы защиты информации требуются профессиональные знания, активная поддержка руководства организации и серьезное финансирование.

В состав системы защиты информации обычно входят следующие компоненты и подсистемы, тесно интегрированные между собой и с другими компонентами ИТ-инфраструктуры:

- Подсистема защиты периметра сети
- Подсистема обеспечения безопасности межсетевых взаимодействий
- Подсистема мониторинга и аудита безопасности
- Подсистема обнаружения и предотвращения атак
- Подсистема резервного копирования и восстановления данных
- Подсистема анализа защищенности и управления политикой безопасности
- Подсистема контроля целостности данных

- Криптографическая подсистема
- Инфраструктура открытых ключей
- Подсистема защиты от вредоносного ПО
- Подсистема фильтрации контента и предотвращения утечки конфиденциальной информации
- Подсистема установки обновлений ПО
- Подсистема администрирования безопасности

Процедура создания и сопровождения системы защиты информации

Процедура создания и сопровождения системы обеспечения информационной безопасности и защиты информации включает в себя следующие этапы:

- Предварительное обследование объекта информатизации с целью определения его текущего состояния, выработки требований по обеспечению безопасности, документирование информационной системы
- Создание Концепции обеспечения информационной безопасности
- Разработка Технического задания
- Техническое проектирование
- Рабочее проектирование (включая документацию на используемые средства защиты, план ввода системы в эксплуатацию и организационно-распорядительных документов по обеспечению информационной безопасности), планирование обучения пользователей и обслуживающего персонала
- Поставка программных и технических средств защиты информации, ввод системы в эксплуатацию, настройка всех компонентов и подсистем, проведение приемо-сдаточных испытаний
- Обучение пользователей и обслуживающего персонала
- Аттестация объекта информатизации по требованиям безопасности информации в системе сертификации ФСТЭК (при необходимости)
- Сопровождение системы, техническая поддержка, аутсорсинг информационной безопасности

Создание концепции информационной безопасности

Создание Концепции обеспечения информационной безопасности обычно предшествует техническому проектированию. Целью создания Концепции является определение основных целей и задач, а также общей стратегии построения системы защиты информации, выработка требований и базовых подходов к их реализации.

Концепция информационной безопасности организации определяет состав критичных информационных ресурсов и основные принципы их защиты. Принципы обеспечения информационной безопасности обуславливают необходимость применения определенных методов и технологий защиты. Определение способов реализации этих принципов путем применения конкретных программно-технических средств защиты и системы организационных мероприятий является предметом конкретных проектов и политик безопасности, разрабатываемых на основе Концепции.

Концепция должна пересматриваться по мере выявления новых методов и технологий осуществления атак на информационные ресурсы. Подобный пересмотр также должен производиться по мере развития информационных систем организации.

Разработка проектной документации

Целью проектирования системы обеспечения информационной безопасности является выработка рекомендаций, организационных и технических решений по обеспечению безопасности информационных ресурсов хранимых, обрабатываемых и передаваемых по каналам связи в компьютерных сетях организации.

Техническое проектирование является необходимым условием для реализации комплексного подхода к обеспечению информационной безопасности. В отсутствие технического проекта возможно лишь реализация фрагментарных мер и механизмов безопасности, за счет которых в современных условиях невозможно решение основных вопросов обеспечения информационной безопасности.

Технический проект системы защиты информации включает в себя:

- Пояснительную записку, содержащую описание основных технических решений по созданию системы и организационных мероприятий по подготовке системы к вводу в действие
- Схемы комплекса технических и программных средств защиты информации
- Спецификацию на комплекс технических средств
- Спецификацию на комплекс программных средств

Рабочий проект помимо этого, включает в себя программно-техническую документацию, инструкции, регламенты и прочие организационно-распорядительные документы по обеспечению информационной безопасности, а также план ввода системы в эксплуатацию.

Заказ услуг

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