СИСТЕМНЫЙ ПОДХОД К УПРАВЛЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

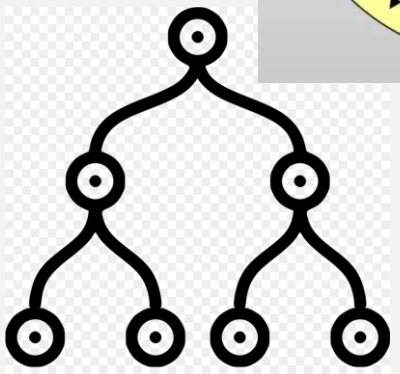
МАРЧУК ИВАН ИУ6-72Б

СИСТЕМНЫЙ ПОДХОД

Способ организации действий, который охватывает любой род деятельности, выявляя закономерности и взаимосвязи с целью их более эффективного использования. При этом он является не столько методом решения задач, сколько методом постановки задач.

ОСНОВНЫЕ ПРИНЦИПЫ СИСТЕМНОГО ПОДХОДА:

- Любая система является подсистемой более сложной системы, которая влияет на структуру и функционирование рассматриваемой;
- Любая система имеет иерархическую структуру, элементами и связями которой нельзя пренебрегать без достаточных оснований;
- При анализе системы необходим учет внешних и внутренних влияющих факторов, принятие решений на основе их небольшого числа без рассмотрения остальных может привести к результатам неотражающим действительность;
- Накопление и объединение свойств элементов системы приводит к появлению качественно новых свойств, отсутствующих у ее элементов.



ЭФФЕКТИВНОСТЬ РЕАЛИЗАЦИИ СИСТЕМНОГО ПОДХОДА

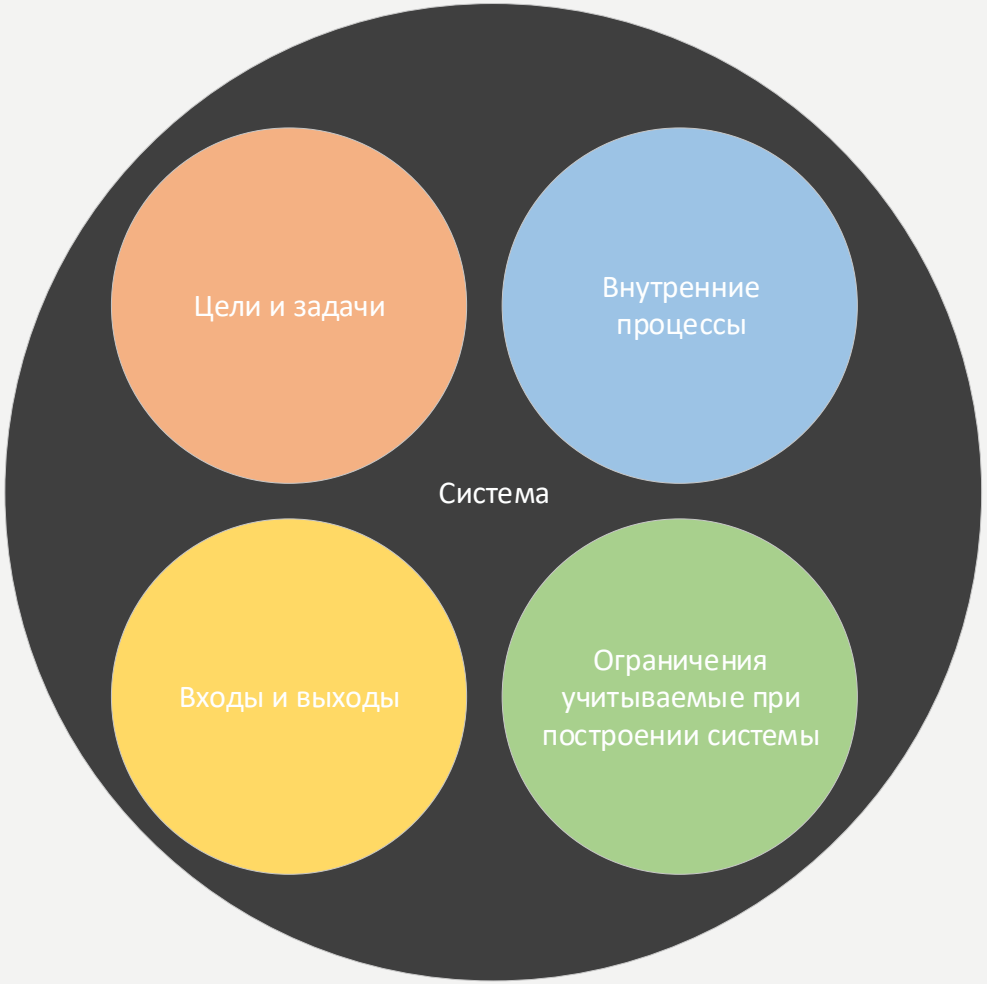
- На практике она зависит от умения специалиста выявлять и объективно анализировать все многообразие факторов и связей достаточно сложного объекта исследования, каким является организация, например, как объект защиты. Необходимым условием такого умения является наличие у специалиста так называемого системного мышления, формируемого в результате соответствующего обучения и практики решения слабо формализуемых проблем. Системное мышление - важнейшее качество не только специалиста по защите информации, но любого организатора и руководителя.

СИСТЕМНАЯ ИНТЕГРАЦИЯ НА ОБЪЕКТЕ ИНФОРМАТИЗАЦИИ

Системная интеграция – это разработка комплексных решений по автоматизации технологических и бизнес-процессов предприятия (организации).

Её конечная цель – максимально эффективное управление технологическими процессами, производством, организацией в целом.

СИСТЕМА ЗАДАЕТСЯ СЛЕДУЮЩИМИ ПАРАМЕТРАМИ:



- Целями и задачами (конкретизированными в пространстве и во времени целями);
- Входами и выходами системы;
- Ограничениями, которые необходимо учитывать при построении (модернизации, оптимизации) системы;
- Процессами внутри системы, обеспечивающими преобразование входов в выходы.

СИСТЕМНОСТЬ И КОМПЛЕКСНОСТЬ ЗАЩИТЫ ИНФОРМАЦИИ

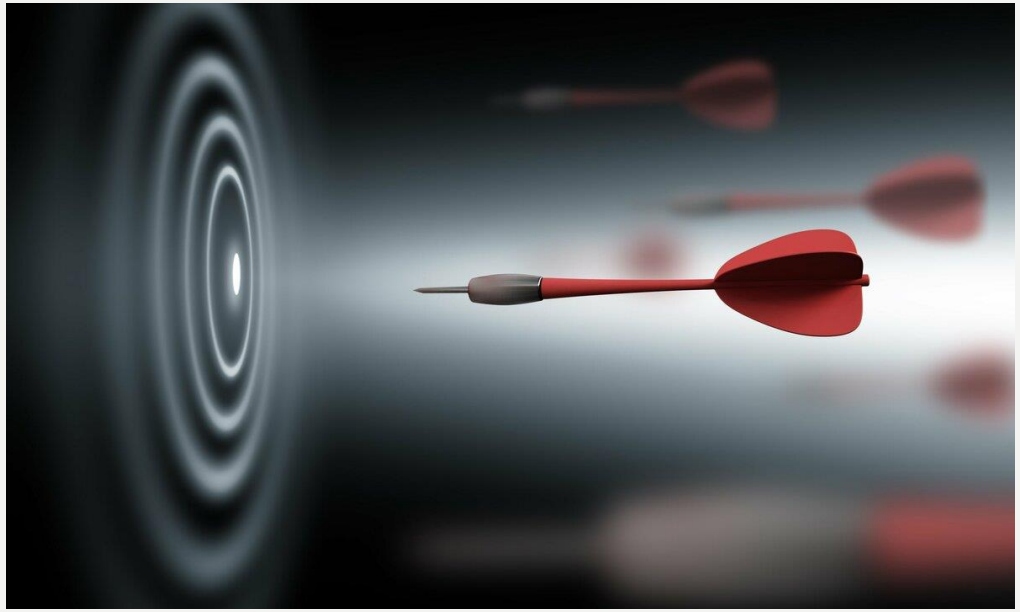
- Решение проблемы информационной безопасности объекта информатизации – системная задача. При этом объект информатизации является объектом защиты информации (объект защиты).
- Рассматриваются все аспекты, связанные с информационной деятельностью на объекте информатизации и с её обеспечением.

ЦЕЛЬ СИСТЕМЫ ЗАЩИТЫ

- Обеспечение требуемых уровней безопасности информации на фирме, в организации, на предприятии (на объекте защиты).

Задачи конкретизируют цели применительно к видам и категориям защищаемой информации, а также элементам объекта зашиты и отвечают на вопрос, что надо сделать для достижения целей.

Кроме того, уровень защиты нельзя рассматривать в качестве абсолютной меры, безотносительно от ущерба, который может возникнуть от потери информации и использования ее злоумышленником во вред владельцу информации.



ВХОДАМИ СИСТЕМЫ ЗАШИТЫ ИНФОРМАЦИИ ЯВЛЯЮТСЯ:

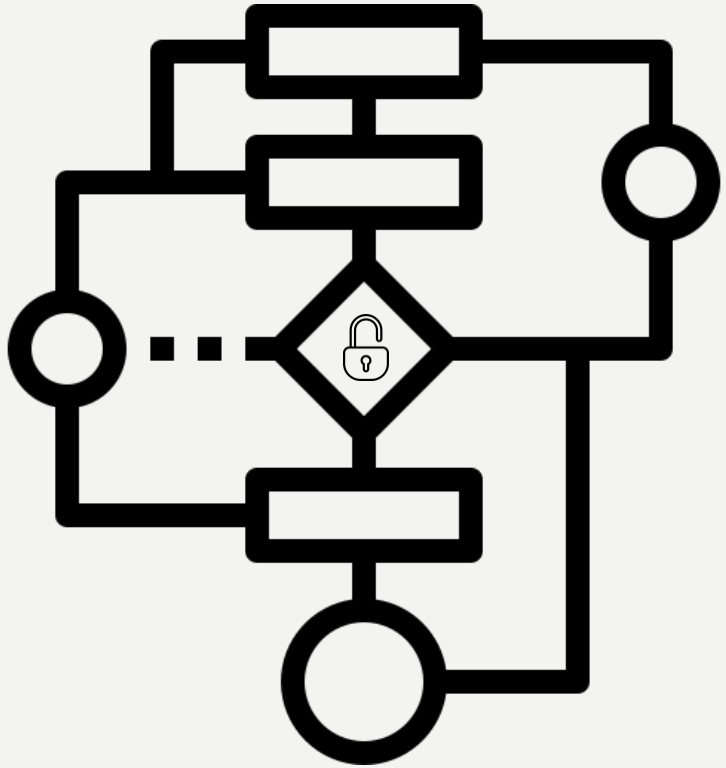
- Воздействия злоумышленников при физическом проникновении к источникам конфиденциальной информации с целью ее хищения, изменения или уничтожения;
- Различные физические поля электрические сигналы, создаваемые техническими средствами злоумышленников и которые воздействуют на средства обработки и хранения информации;
- Стихийные силы, прежде всего, пожары, приводящие к уничтожению или изменению информации;
- Физические поля и электрические сигналы с информацией, передаваемой по функциональным каналам связи;
- Побочные электромагнитные и акустические поля, а также электрические сигналы, возникающие в процессе деятельности объектов защиты и несущие конфиденциальную информацию.

Выходами системы защиты являются меры по защите информации, соответствующие входным воздействиям.

СОЗДАНИЕ МЕР ЗАЩИТ

Алгоритм процесса преобразования входных воздействий (угроз) в меры защиты определяет вариант системы защиты. Вариантов, удовлетворяющих целям и задачам, может быть много. Сравнение вариантов производится по количественной мере, называемой критерием эффективности системы. Критерий может быть в виде одного показателя, учитывающего основные характеристики системы или представлять собой набор частных показателей. Единый общий критерий эффективности называется глобальным.

В качестве частных показателей критерия эффективности системы защиты информации используются, в основном, те же. что и при оценке эффективности разведки. Это возможно потому, что цели и задачи, а, следовательно, значения показателей эффективности разведки и защиты информации близки по содержанию, но противоположны по результатам. То, что хорошо для безопасности информации, плохо для разведки, и наоборот.



ПОКАЗАТЕЛИ ЭФФЕКТИВНОСТИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

- Вероятность обнаружения и распознавания органами разведки объектов защиты;
- Погрешности измерения признаков объектов защиты;
- Достоверность (вероятность ошибки) дискретного элемента информации (буквы, цифры, элемента изображения).

Очевидно, что система защиты тем эффективнее, чем меньше вероятность обнаружения и распознавания объекта защиты органом разведки (злоумышленником), чем ниже точность измерения им признаков объектов защиты, ниже разборчивость речи, выше вероятность ошибки приема органом разведки дискретных сообщений.

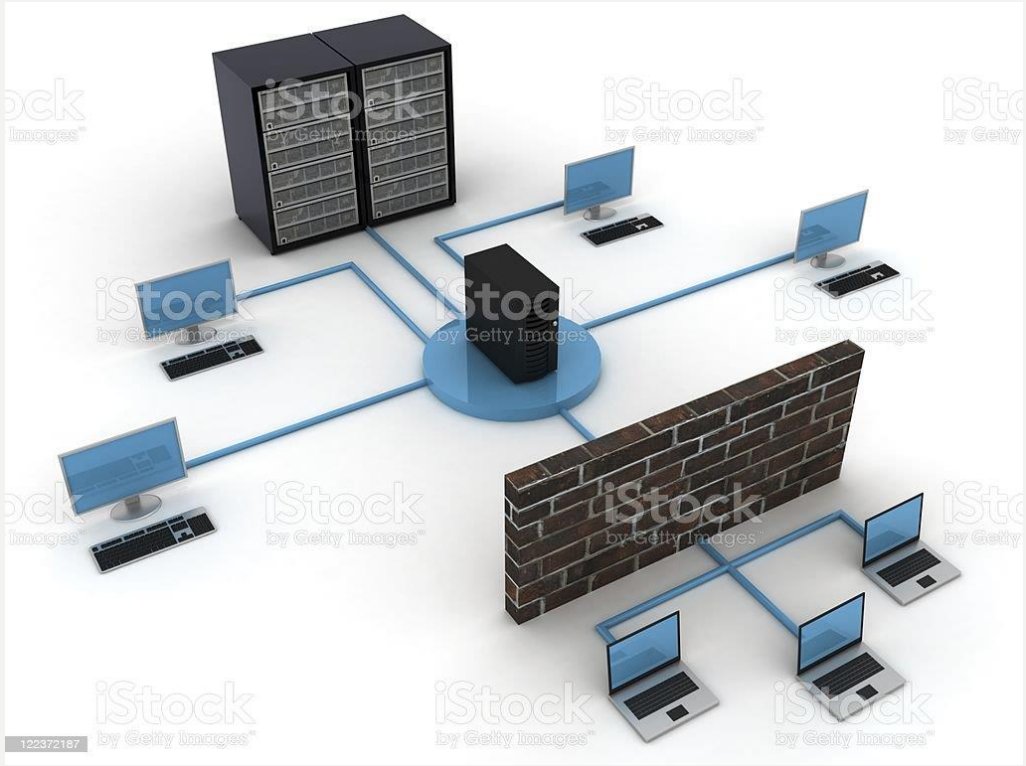
ПРИНЦИП СИСТЕМНОСТИ

При декомпозиции целей и синтезе структурных элементов КСЗИ между ними, компонентами АС и процессами реализации информационных технологий, в интересах которых осуществляется защита информации, должны быть установлены такие связи, которые обеспечивают цельность КСЗИ и её взаимодействие с другими системами объекта информатизации и подсистемами АС. Системность и комплексность обеспечивается путём создания комплексных систем защиты информации (КСЗИ).

ПРИНЦИП КОМПЛЕКСНОСТИ

Оптимальное использование различных методов, мер и средств защиты информации (административно-правовых, организационных, организационно-технических, технических, программных) для нейтрализации угроз информации и поддержания заданного уровня защищённости информации, интеграции этих средств в единую технологически связанную и управляемую систему.

ПРИ ЭТОМ ОБЕСПЕЧИВАЕТСЯ:



- Рассмотрение всех выявленных при обследовании угроз информации, влияющих на состояние защищённости информации в АС и на объекте информатизации;
- Выделение актуальных из них путём анализа порождаемых ими рисков и последующего возможного ущерба, если риск становится реальным событием;
- Ранжирование актуальных угроз;
- Учёт всех выделенных актуальных угроз при создании КСЗИ.

ВСЁ!