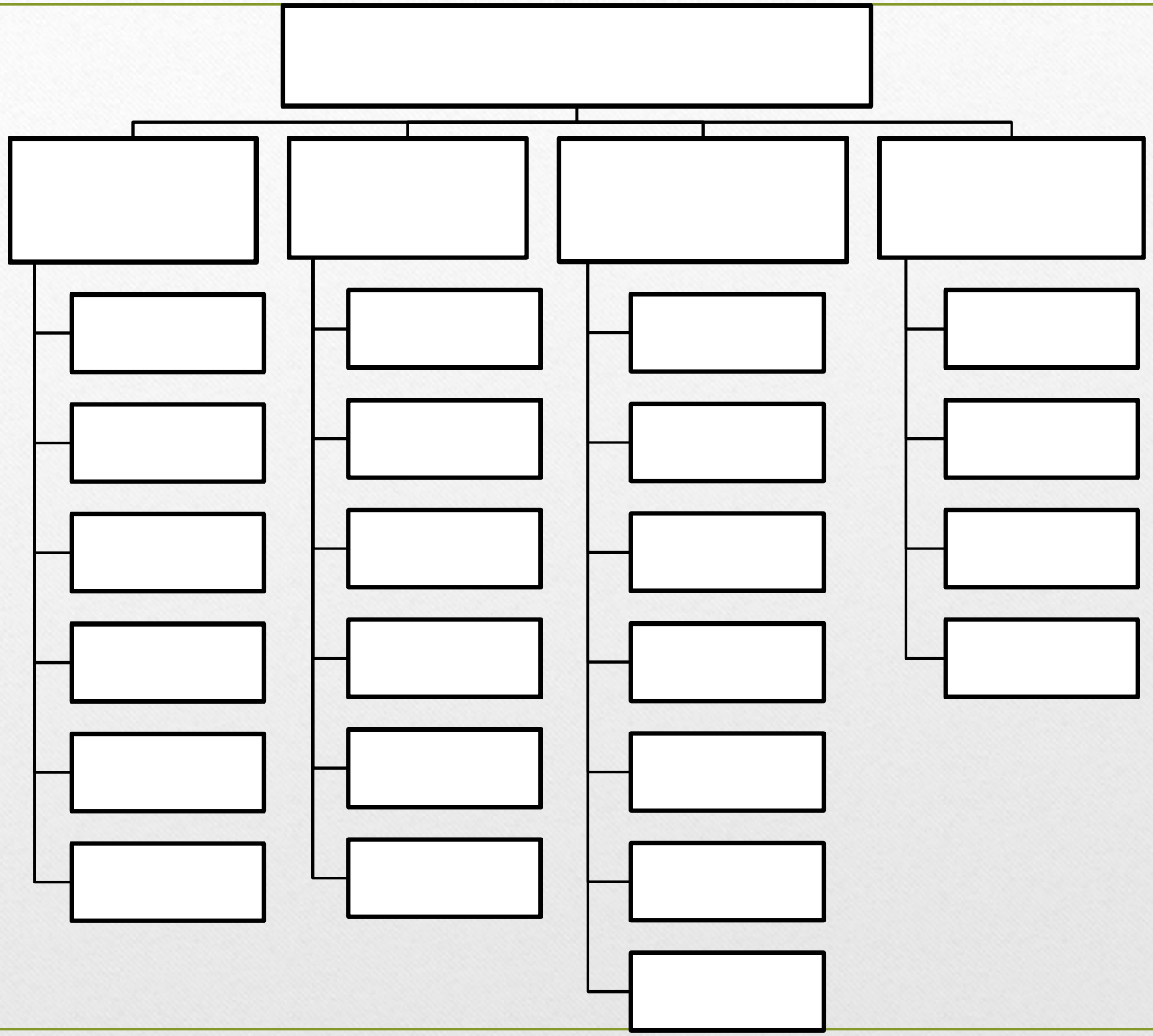
Методы обнаружения аномалий

В современном мире при стремительном развитии информационно-телекоммуникационных систем и сетей вопросы безопасности становятся наиболее актуальными. В связи с увеличением объема информационного потока вопрос обнаружения, диагностики и дальнейшего мониторинга сетевых аномалий является одной из главных задач информационного общества

В настоящее время методы обнаружения аномалий разделяются на следующие категории:

- Поведенческие методы;
- Методы машинного обучения;
- Методы вычислительного характера;
- Методы, основанные на знаниях.
- В свою очередь эти категории делятся на подклассы



Система обнаружения вторжений (СОВ) – программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими в основном через Интернет. Соответствующий английский термин – Intrusion Detection System (IDS).

Системы обнаружения вторжений используются для обнаружения некоторых типов вредоносной активности, которая может нарушить безопасность компьютерной системы. К такой активности относятся сетевые атаки против уязвимых сервисов, атаки, направленные на повышение привилегий, неавторизованный доступ к важным файлам, а также действия вредоносного программного обеспечения (компьютерных вирусов, троянов и червей)

Архитектура СОВ включает:

– сенсорную подсистему, предназначенную для сбора событий, связанных с безопасностью защищаемой системы;

– подсистему анализа, предназначенную для выявления атак и подозрительных действий на основе данных сенсоров;

– хранилище, обеспечивающее накопление первичных событий и результатов анализа;

– консоль управления, позволяющая конфигурировать СОВ, наблюдать за состоянием защищаемой системы и СОВ, просматривать выявленные подсистемой анализа инциденты

Современные методы обнаружения вторжений базируются на нескольких основных принципах:

Сигнатурный: описывают каждую атаку особой моделью или сигнатурой, в качестве которой могут применяться строка символов, семантическое выражение на специальном языке, формальная математическая модель

Поведенческий (обнаружение аномалий): базируются не на моделях информационных атак, а на моделях штатного функционирования ИС. Принцип работы любого из таких методов состоит в обнаружении несоответствия между текущим режимом работы ИС и режимом работы, отвечающим штатной модели данного метода. Любое несоответствие рассматривается как информационная атака. Преимущество методов данного типа – возможность обнаружения новых атак без модификации или обновления параметров модели.

Комбинированные методы – методы продукционных правил, позволяют описывать модели атак на естественном языке с высоким уровнем абстракции.

Экспертные системы, использующие данные методы, состоят из двух баз данных: фактов и правил. Факты представляют собой исходные данные о работе ИС, а правила – алгоритмы логических решений о факте атаки на основе поступившего набора фактов.