**Искусственный интеллект**

Существует слабый ИИ (решение 1 задачи, интеллект не имеет творческой части, не мыслит, как человек) и сложный ИИ (мульти-задачный, мыслит, как человек, имеет творческую составляющую).

ИИ в кибербезопасности обрабатывает огромные объёмы данных, учится анализировать угрозы, предугадывать их возможное изменение, находить угрозы и предпринимать активные действия по их устранению.

Наиболее опасной атакой для сети есть вторжение вируса в 1 ПК, и подальшее заражение всех ПК в сети.

**Intrusion Detection System (IDS) -** программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими в основном через Интернет.

IDS на основе ИИ имеет 3 типа работы:

- Static – использует стандартные, общепризнанные меры защиты.

- All Based – использует всевозможные меры зашиты (нейронные сети, непарная логика и.т.д.)

- Knowledge based – использует меры защиты, которому обучили данные интеллект.

В данном документе будет рассматриваться именно All-Based IDS with AI.

**Нейронная сеть**

Нейронная сеть работает по типу человеческого мозга. Она состоит из множества узлов и связей между ними (нейронов). Между входящими данными и выходящими есть несколько уровней нейронов, связанных между собой и между уровнями.

Преимущество НС заключается в том, что она может сделать вывод о нормальном или ненормальном поведении пользователей исходя лишь из обработанных данных в самой сети, без заведомо установленных правил.

Также преимуществом НС является высокая скорость обнаружения вторжения и последующих действий. При обнаружении конкретной ошибки, в будущем она больше не сможет пройти защиту НС.

**Нечёткая логика**

Нечёткая логика основана на правилах поведения системы/пользователя, переведённые в математические эквиваленты, заведомо указанных её человеком. Решение IDS может находится в диапазоне от 0 до 1, от полностью ложного до полностью верного соответственно. Наиболее продуктивным IDS будет подход объединения нечёткой логики с нейронной сетью: нечёткая логика задаст определенные правила нарушения в системе, а нейронная сеть будет обучать IDS возможным атакам, для их предотвращения в будущем.

**Генетический алгоритм**

Генетический алгоритм схож с естественным отбором в природе. Сначала формируется первая партия «хромосом», которая методом подбора пытается выявить реальную угрозу вторжения в сеть, либо же предпринять действия по её устранению. Те «хромосомы», которые правильно вычислят угрозу (в том числе и определят ложная она или нет) будут «размножаться» и их потомство уже будет владеть всеми навыками своих родителей. Тем самым, это потомство уже будет иметь чёткие правила по обнаружению и борьбе с угрозами, а также дальше учиться выявлять новые угрозы, сравнивать их с уже известными им, предугадывать будущие угрозы, с модифицированным шаблоном. Далее цикл продолжается, и они создают следующее потомство с уже более обширной базой знаний и навыков.

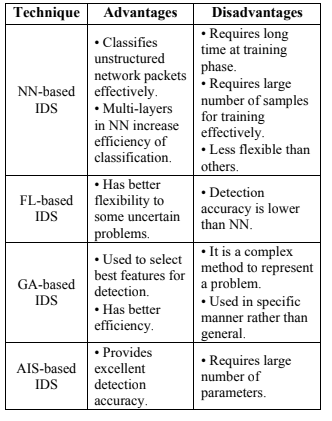
Генетический алгоритм после стадии обучения имеет высокую продуктивность, скорость обнаружения и точность выявления угроз.

**Искусственная иммунная система**

Пример иммунной биологической системы переведенный в математические модели. В систему IDS сначала вносятся нормальные протоколы поведения системы/пользователя. Детекторы иммунной системы сравнивают поведение с установленным протоколом нормального поведения, т.е. применяется алгоритм отрицательного выбора. Если в таком сравнении присутствуют отклонения, то детектор блокирует угрозу, в противном случае пропускает. Таким образом незрелые детекторы запоминают шаблоны отклонений от нормы и в будущем уже не пропустят угрозу вторжения в систему или сеть.

Для улучшения ИИС предлагается ввести также алгоритм положительного выбора, чтобы сохранять образцы(шаблоны) нормального поведения, что приведёт к более быстрому обучению системы, а также более точной классификации угрозы.

**Таблица со сравнительным анализом всех перечисленных алгоритмов для IDS**

****