В.А.ВИШНЯКОВ[1], М.Г.МОЗДУРАНИ ШИРАЗ[2]

ПРОТИВОДЕЙСТВИЕ УГРОЗАМ В ИНТЕГРИРОВАННОЙ КОРПОРАТИВНОЙ СИСТЕМЕ УПРАВЛЕНИЯ С ИСПОЛЬЗОВАНИЕМ ГЕНЕТИЧЕСКИХ АЛГОРИТМОВ

[1]*Учреждение образования «Белорусская государственная академия связи», г. Минск, Республика Беларусь*

[2]*Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г.Минск, Республика Беларусь*

В докладе представлено введение в системы обнаружения атак (IDS), с тем чтобы дать подробную информацию об их преимуществах, месте использования и недостатках [1].. Затем сделано краткое разъяснение генетических алгоритмов, включая: их типы, функцию пригодности, генетические операторы, такие как кроссовер выборок, мутация, определение размера популяции, длину хромосомы, мутацию и скорость кроссовера.

Поскольку набор данных, используемый в докладе является набором KDD99, было проведено его краткое исследование с перечислением атак и анализа структуры набора данных KDD99. Было выведено множество вероятностных распределений относительно атак и их классов (DOS, PROBE, R2L, U2R).

Применяя меры теории информации, такие как энтропия и взаимная информация, функция связи были ранжированы после процесса нормализации в соответствии с каждым классом атаки. Такое ранжирование позволяет уменьшить вычислительную сложность путем выбора наиболее важных функций для каждого класса атаки. Выбор характеристик доказал что они уменьшили скорость обнаружения. Кроме того, доказано, что запуск некоторых моделей обнаружения, таких как SF-5NN и SUS-5NN, с использованием нескольких выбранных функций более эффективен, чем запуск его с полным набором из 41 функции. Это связано с тем, что некоторые функции не имеют отношения к задаче обнаружения и могут замедлять процесс.

Были предложены два подхода обнаружения атаки, основанные на лучших выбранных функциях и алгоритмах K-NN, SF-KNN и SUS-KNN. Эти подходы обеспечили хорошие коэффициенты классификации, равные 92,56%, 92,84% и коэффициенты погрешности 2%, 4,52% соответственно. Предложенные модели лучше, чем многие другие подходы, такие как традиционные 5-NN, C4.5, C5 особенно в обнаружении опасных атак, таких как U2R и R2L. Кроме того, эти модели могут обнаруживать все типы известных и неизвестных атак, кроме атак "phf" и "mailbomb". Недостатком SF-KNN и SUS-KNN является их вычислительная сложность, так как для того, чтобы решить, является ли соединение нормальным или нет, его необходимо сравнить с 494021 ссылочными соединениями.

Данная работа нацелена на поиск атак с использованием аппарата генетических алгоритмов (ГА) для построения классификаторов трафика сети, которые называются ГАКТ. С помощью ГА был разработан линейный классификатор, использующий пять лучших функций. Известный тариф классификации 92,82%, а новый тариф обнаружения составил 94,89% который лучшее чем результаты с другими подходами. Лучший результат получен при обнаружении атак типа R2L (30,30%), с учетом, что атаки R2L трудно обнаружить.

ЛИТЕРАТУРА

1. Вишняков, В. А. Информационная безопасность в корпоративных системах, электронной коммерции и облачных вычислениях: методы, модели, программно-аппаратные решения. Монография. / В. А. Вишняков. – Минск: , 2016. – 276 с.