УДК 004

ОБЗОР АЛГОРИТМОВ ВЫЯВЛЕНИЯ СЕТЕВЫХ АТАК

Тремасова У.В., студентка 3 курса экономического факультета
Научный руководитель – Голубев С.В., к.э.н., доцент
ФГБОУ ВО Ульяновский ГАУ

***Ключевые слова**: Сетевая атака, анализ, информационная система, алгоритм.*

В статье приведены алгоритмы выявления сетевых атак. Рассмотрен так же термин «сетевой атаки». Приведен анализ четырех наиболее распространенных алгоритмов выявления сетевых атак. Выделены основные характеристики, достоинства и недостатки алгоритмов.

Сетевая атака - это действия с применением программных и (или) технических средств и с использованием сетевого протокола, направленные на реализацию угроз несанкционированного доступа к информации, воздействия на нее или на ресурсы автоматизированной информационной системы.

Анализ литературных источников показывает, что существует множество алгоритмов для выявления атак в сети. В настоящее время основными алгоритмами выявления сетевых атак являются:

1. Алгоритм на основе дискретного вейвлет-преобразования;
2. Алгоритм Бродского-Дарховского;
3. Алгоритм на основе сумме квадратов вейвлет-коэффициентов;
4. Алгоритм на основе максимума квадратов вейвлет-коэффициентов.

По данным исследования, проведённого аналитическим агентством 42Future по заказу Qrator Labs, в конце 2015 года, 25% крупнейших ритейлеров сталкивались с DDoS за последний год. Количество атак на сайты ритейлеров возросло примерно на 70% по сравнению с 2014 годом.

Как сообщили 80% опрошенных, по их мнению атаки в первую очередь заказывают конкуренты. Вторая причина организации атак — вымогательство путём шантажа; так ответили 45% опрошенных.

Алгоритм выявления сетевых атак:

1. Алгоритм на основе дискретного вейвлет преобразования с применением статистических критериев.

Режим алгоритма: Критерий Фишера и Критерий Кохрана.

В данном алгоритме используется техника скользящих окон W1 и W2, позволяющая увеличить надёжность обнаружения незначительных аномалий, свидетельствующих о наличии сетевой атаки. Достоинства данного алгоритма: атака хорошо обнаруживается на каждом уровне БВП декомпозиции (критерий Фишера обнаруживает атаку наиболее явно). Недостатки данного алгоритма: при начальном уровне разложения обнаруживает наибольшее количество атак, но некоторые аномалии могут быть пропущены, если начать разложение с более старших уровней. На старших уровнях повышается количество возникновения ложных тревог.

2. Алгоритм обнаружения аномалий Бродского-Дарховского.

Режим алгоритма: Стандартный режим и режим скользящих окон.

При выборе стандартного режима особое влияние проявляют шумы. При выборе алгоритма в режиме скользящего окна совокупное действие помех уменьшается, и выбросы, характеризующие начало и конец воздействия, представляются в более явном виде. Для практической реализации лучше использовать алгоритм в режиме скользящего окна.

3. Алгоритм, основанный на сумме квадратов вейвлет-коэффициентов.

Режим алгоритма: Выявление аномалий с использованием вейвлета Хаара и выявление аномалий с использованием вейвлета Добеши.

Алгоритм обладает большой эффективностью. Наибольший эффект обнаруживается при использовании коэффициентов аппроксимации для вейвлетов Хаара на верхних уровнях разложения. Но увеличение размера окна анализа может привести к возрастанию вероятности правильного обнаружения аномалии, но при этом возрастает вероятность ложного обнаружения.

4. Алгоритм, основанный на максимуме квадратов вейвлет-коэффициентов.

Режим алгоритма: Алгоритм с использованием вейвлета Хаара и алгоритм с использованием вейвлета Добеши.

Алгоритм обладает меньшей эффективностью, чем алгоритм, основанный на сумме квадратов вейвлет-коэффициентов. Наиболее информативно отражают атаку в этом алгоритме коэффициенты аппроксимации с использование вейвлета Хаара.

Приведённые выше алгоритмы анализируют следующие параметры: ошибки первого рода, ошибки второго рода, количество пра-

вильно обнаруженных аномалий. Таким образом, по результатам проведенного анализа можно сделать вывод о том, что наиболее простыми в реализации являются алгоритм Бродского-Дарховского и алгоритм на основе дискретного вейвлет-преобразования с применением статистических критериев. Наиболее точным в обнаружении аномалий является алгоритм Бродского-Дарховского. При его использовании обнаруживается меньше ошибок 1-ого и 2-ого рода, чем при использовании алгоритма на основе дискретного вейвлет-преобразования с применением статистических критериев. Алгоритм Бродского-Дарховского имеет наибольшее количество правильно обнаруженных аномалий, но при этом имеет большие требования к ресурсам.

Библиографический список

1. ГОСТ Р 53114 - 2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. - М.: ИПК Издательство стандартов, 2008.
2. Шелухин, О.И. Обнаружение DOS и DDOS-атак методом дискретного вейвлет-анализа / О.И. Шелухин, Ю.А. Иванов, В.Ю. Ригов // T-Comm - Телекоммуникации и Транспорт. - 2011. - №1. - С. 44-46.
3. Шелухин, О.И. Обнаружение сетевых аномальных выбросов трафика методом разладки Бродского-Дарховского / О.И. Шелухин, А.С. Филинова // T-Comm - Телекоммуникации и Транспорт. - 2013.- №10. - С. 116-118.

OVERVIEW OF ALGORITHMS FOR DETECTION OF NETWORK ATTACKS

Tremasova U.V.

Keywords: *Network attack, analysis, information system, algorithm.*

The article presents algorithms to detect network attacks. Considered as the term "network attack". The analysis of the four most common algorithms for detection of network attacks. Main characteristics, advantages and disadvantages of the algorithms.