УДК 004.056.53

СОВРЕМЕННЫЕ СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В КОМПЬЮТЕРНЫХ СЕТЯХ

М.М. Каримов, М.М. Кадыров, С.М. Сагатова (ТашГТУ)

В статье рассматриваются структура и классификация современных систем обнаружения вторжений в компьютерных сетях. Характеризуются основные направления распознавания нарушений безопасности защищаемых систем в современных СОВ. Выполнен анализ используемых методов и моделей структуры СОВ в соответствии с выделенными основными группами. Особое внимание в статье уделяется анализу методов обнаружения аномалий и злоупотреблений. Приведены основные недостатки существующих систем обнаружения вторжений и обоснованы направления их совершенствования.

We consider the structure and classification of modern intrusion detection systems. Characterized by the main directions of the recognition of security breaches protected systems in modern intrusion detection systems. The analysis of the methods and models of the intrusion detection systems in accordance with the selected major groups. Particular attention is paid to the methods of detection of anomalies and irregularities. The main disadvantages of the existing intrusion detection systems and the directions of their improvement.

Мақолада замонавий суқилиб киришни аниқлаш тизимлари таркиби кўриб чиқилган. Асосий химояланган тизимларда замонавий сукулиб киришларни йўналишлари тавсифланган. Қўлланилган усуллар ва моделлар суқилиб киришни аниқлаш тизимлари таркибини ажратилган гурухлар асосида тахлил қилинган. Мақолада тармоқ фаолиятини нормадан четга чиқиши ва фойдаланувчиларни сушистеъмол қилишларини аниқлаш усулларига алоҳида эътибор берилган. Мавжуд бўлган суқилиб киришни аниқлаш тизимлари асосий камчиликлари ва уларни такомилаштириш йўналишлари берилган.

Ключевые слова: *безопасность компьютерных сетей, обнаружения вторжений, обнаружения злоупотреблений, обнаружения аномалий, подсистема, датчики.*

Прогресс компьютерных и информационных технологий, рост масштабов компьютерных сетей, усложнение их структуры и увеличение нагрузки на них, а также рост числа различных вредоносных программ диктуют необходимость повышения безопасности компьютерных сетей. Среди многих методов, таких как методы аутентификации, шифрования данных, брандмауэры, использование СОВ имеет важное значение для защиты от атак.

Вторжение определяется как набор действий, направленных на нарушение целостности, конфиденциальности и доступности некоторого компьютерного ресурса. Обнаружение вторжений — это процесс мониторинга и анализа событий, происходящих в компьютерной системе, с целью поиска признаков проблем безопасности.

Первые модели прототипы систем обнаружения вторжений использовали анализ данных аудита компьютерных систем[1].

До недавнего времени наиболее распространенной структурой СОВ была модель, предложенная Дороти Деннинг (D. Denning) [2].

В современных системах обнаружения логически вторжений (рис 1.1.) выделяют следующие основные элементы: подсистему сбора информации, подсистему анализа и модуль представления данных [3].

Подсистема сбора информации аккумулирует данные о работе защищаемой системы. Для сбора информации используются автономные модули – датчики. Количество используемых датчиков различно и зависит от специфики защищаемой системы. Датчики в СОВ принято классифицировать по характеру собираемой информации. В соответствии с общей структурой информационных систем выделяют следующие типы:

- датчики приложений – данные о работе программного обеспечения защищаемой системы;
- датчики хоста – функционирование рабочей станции защищаемой системы;
- датчики сети – сбор данных для оценки сетевого трафика;
- межсетевые датчики – содержат характеристики данных, циркулирующих между сетями.

Система обнаружения вторжения может включать любую комбинацию из приведенных типов датчиков.

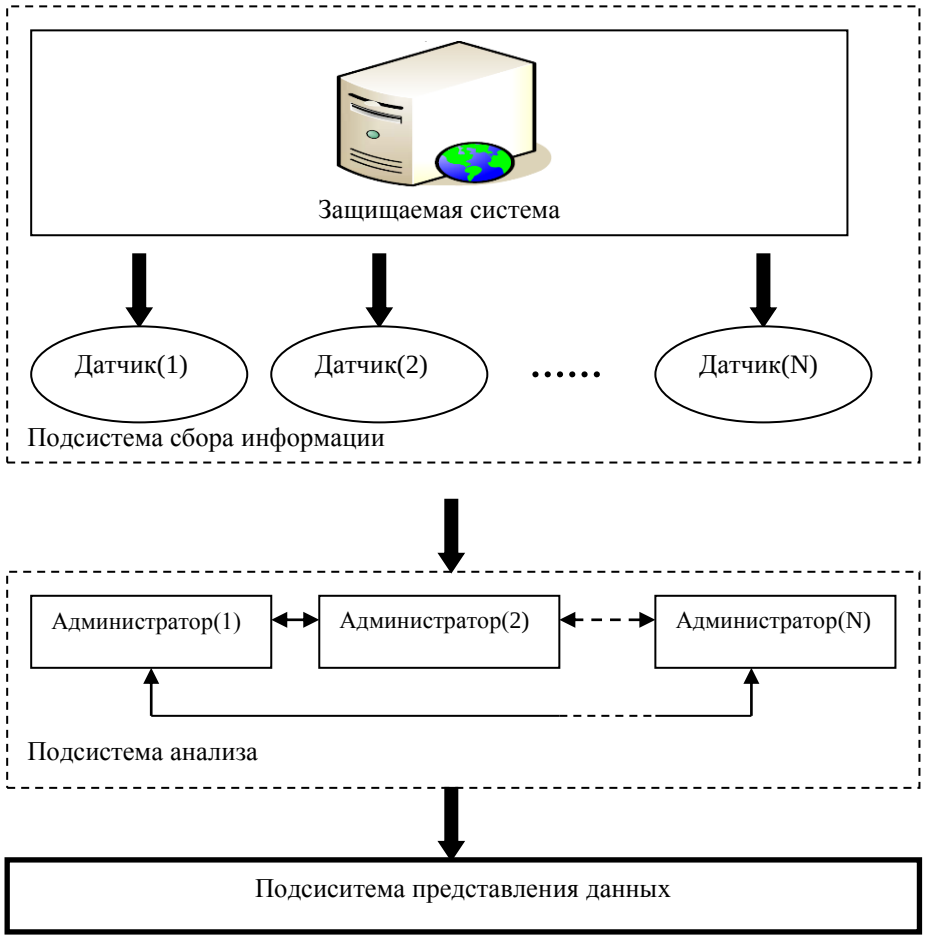

Рис. 1.1. Общая структура системы обнаружения вторжения

Подсистема анализа структурно состоит из одного или более модулей анализа – анализаторов. Наличие нескольких анализаторов требуется для повышения эффективности обнаружения. Каждый анализатор выполняет поиск атак или вторжений определенного типа. Входными данными для анализатора является информация из подсистемы сбора информации или от другого анализатора. Результат работы подсистемы – индикация о состоянии защищаемой системы.

Подсистема представления данных необходима для информирования заинтересованных лиц о состоянии защищаемой системы. В некоторых системах предполагается наличие групп пользователей, каждая из которых контролирует определенные подсистемы защищаемой системы. Поэтому в таких СОВ применяется разграничение доступа, групповые политики, полномочия и т.д.

СОВ динамически отслеживает события, происходящие в системе, и решает, являются ли эти события симптомом нападения или являются естественным использованием системы [3].

В основу классификации систем обнаружения вторжений могут быть положены следующие понятия: подход, источник информации, структура, реакция.

Существуют два подхода к обнаружению вторжений [3]:

- обнаружение злоупотреблений (Misuse Detection);
- обнаружение аномалий (Anomaly Detection).

Анализ методов обнаружения аномалий

Методы обнаружения аномалий направлены на выявление неизвестных атак и вторжений. Для защищаемой системы СОВ на основе совокупности параметров оценки формируется «образ» нормального функционирования. В современных СОВ выделяют несколько способов построения «образа»:

- накопление наиболее характерной статистической информации для каждого параметра оценки;
- обучение нейронных сетей значениями параметров оценки;
- событийное представление.

Легко заметить, что в обнаружении очень значительную роль играет множество параметров оценки. Поэтому в обнаружении аномалий одной из главных задач является выбор оптимального множества параметров оценки.

Выбор оптимальной совокупности признаков оценки защищаемой системы: В настоящие время используется эвристическое определение (выбор) множества параметров измерений защищаемой системы, использование которого должно дать наиболее эффективное и точное распознавание вторжений. Сложность выбора множества можно объяснить тем, что составляющие его подмножества зависят от типов обнаруживаемых вторжений. Поэтому одна и та же совокупность параметров не будет адекватной для всех типов вторжений.

Получение единой оценки состояния защищаемой системы.

Общая оценка аномальности должна определяется из расчета множества параметров оценки. Один из возможных методов – использование статистики Байеса. Другой способ, применяемый в (NIDES), основан на использовании ковариантных матриц.

При использование статистики Байеса

Рассматриваются A_1 .. A_n – n измерений, для определения факта вторжения в любой момент времени. Достоверность и чувствительность каждого измерения определяется показателями

$$P(A_i = 1 \mid I) u P(A_i = 1 \mid \neg I) \qquad (1)$$

где I-гипотеза в системе имеются процессы вторжения.

Вероятность вычисляется при помощи теоремы Байеса.

$$P(I \mid A_1, A_2, .., A_n) = P(A_1, A_2, .., A_n \mid I) \frac{P(I)}{P(A_1, A_2, .., A_n)} \quad (2)$$

Для событий I и ¬I, необходимо вычислить условную вероятность для каждой возможной комбинации множества измерений. При этом использованы следующие соотношения:

$$P(A_1, A_2, .., A_n \mid I) = \prod_{i=1}^{n} P(A_i \mid I) \quad (3)$$

и

$$P(A_1, A_2, .., A_n \mid \neg I) = \prod_{i=1}^{n} P(A_i \mid \neg I) \quad (4)$$

Отсюда

$$\frac{P(A_1, A_2, .., A_k \mid I)}{P(A_1, A_2, .., A_k \mid I)} = \frac{P(I) \prod_{i=1}^{n} P(A_i \mid I)}{P(I) \prod_{i=1}^{n} P(A_i \mid I)} \quad (5)$$

Недостаток этого метода является, для получения более реалистичной оценки P(I|A1..An), необходимо учитывать влияние измерений Ai друг на друга.

Анализ методов обнаружения злоупотреблений

Обнаружение вторжений-злоупотреблений основывается на прогностическом определении атак и последующим наблюдением за их появлением. В отличие от обнаружения аномалии, где образ – это модель нормального поведения системы, при обнаружении злоупотребления он необходим для представления несанкционированных действий злоумышленника. Такой «образ» применительно к обнаружению злоупотреблений называется сигнатурой вторжения. Формируется сигнатура на основе тех же входных данных, что и при обнаружении аномалий, то есть на значениях параметров оценки. Сигнатуры вторжений определяют окружение, условия и родство между событиями, которые приводят к проникновению в систему или любым другим злоупотреблениям. Они полезны не только при обнаружении вторжений, но и при выявлении попыток совершения незаконных действий. Частичное совпадение сигнатур может означать, что в защищаемой системе имела место попытка вторжения.

Использование условной вероятности

Для определения злоупотреблений нужно определить условную вероятность

P(Вторжение|Патерн событий)

То есть, другими словами, определяется вероятность того, что какие-то множество или множества событий являются действиями злоумышленника.

Далее используется формула Байеса

$$P(I \mid A_1, A_2, .., A_n) = P(A_1, A_2, .., A_n \mid I) \frac{P(I)}{P(A_1, A_2, .., A_n)} \quad (6)$$

где I – вторжение, а A1… An – последовательность событий. Каждое событие – это совокупность параметров оценки защищаемой системы.

Продукционные/Экспертные системы

Главное преимущество использования продукционных систем заключается в возможности разделения причин и решений возникающих проблем.

В этом случае система кодирует информацию о вторжениях в правилах вида if(если) причина then(то) решение, причем при добавление правил причина соответствует событию(ям), регистрируемых подсистемой сбора информации СОВ. В части (if) правила кодируются условия (причины), необходимые для атаки. Когда все

условия в левой части правила удовлетворены, выполняется действие (решение), заданное в правой его части.

Основные проблемы приложений, использующих данный метод, которые обычно возникают при их практическом применении:

недостаточная эффективность при работе с большими объемами данных;

трудно учесть зависимую природу данных параметров оценки.

При использовании продукционных систем для обнаружения вторжений можно установить символическое проявление вторжения при помощи имеющихся данных.

Таким образом, недостатки современных систем обнаружения можно разделить на две группы – недостатки, связанные со структурой СОВ, и недостатки, относящиеся к реализованным методам обнаружения.

Недостатки структур СОВ.

- Отсутствие общей методологии построения.
- Часто методы системы пытаются обнаружить любую понятную атаку, что приводит к ряду неудовлетворительных последствий.
- До сих пор большинство СОВ создается для использования на конкретном оборудовании, и достаточно трудно использовать их в другой системе, где требуется реализовать похожую политику безопасности.
- Очень сложно обновить существующие системы новыми технологиями обнаружения. Производительность и вспомогательные тесты – трудно оценить производительности СОВ в реальных условиях.
- Отсутствие хороших способов тестирования.

Недостатки методов обнаружения:

1. недопустимо высокий уровень ложных срабатываний и пропусков атак;
2. слабые возможности по обнаружению новых атак;
3. большинство вторжений невозможно определить на начальных этапах;
4. трудно, иногда невозможно, определить атакующего, цели атаки;
5. отсутствие оценок точности и адекватности результатов работы;
6. невозможно определять «старые» атаки, использующие новые стратегии;

Дальнейшие направления совершенствования связаны с внедрением в теорию и практику СОВ общей теории систем, методов теории синтеза и анализа информационных систем и конкретного аппарата теории распознавания образов, так как эти разделы теории дают конкретные методы исследования для области систем СОВ.

На основе изложенного можно сделать вывод о том, что в практической деятельности накоплен значительный опыт решения проблем обнаружения вторжений. Применяемые СОВ в значительной степени основаны на эмпирических схемах процесса обнаружения вторжений, дальнейшее совершенствование СОВ связано с конкретизацией методов синтеза и анализа сложных систем, теории распознавания образов в применении к СОВ.

Литература

1. Wu S. X., Banzhaf W. The use of computational intelligence in intrusion detection systems: A review // Applied Soft ,Computing. 2010. V. 10. P. 1 —35.
2. D. Denning, An Intrusion Detection Model. // IEEE Transactions on Software Engineering, v. SE-13, № I, 2001, pp. 222-232.
3. http://citforum.ru/security/internet/ids_overview/

MODERN INTRUSION DETECTION SYSTEMS IN COMPUTER NETWORKS

Karimov M.M. Kadirov M.M., Sagatova S.M.

СОВРЕМЕННЫЕ СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В КОМПЬЮТЕРНЫХ СЕТЯХ

Каримов М.М. Кадыров М.М., Сагатова С.М.

КОМПЬТЕР ТАРМОҚЛАРИДА ЗАМОНАВИЙ СУҚУЛИБ КИРИШНИ АНИҚЛАШ ТИЗИМЛАРИ

Каримов М.М. Кадыров М.М., Сагатова С.М.