УДК 681.3.067

Г.В. Кузнецов, А.М.Иванов

КЛАССИФИКАЦИЯ И АНАЛИЗ СИСТЕМ И МЕТОДОВ ОБНАРУЖЕНИЯ АТАК

Актуальность исследований в области защиты информации в компьютерных сетях вызвана значительным увеличением за последние годы количества инцидентов, связанных с нарушением политики безопасности организаций (рис. 1).

Системы обнаружения атак появились сравнительно недавно и являются одной из составляющих системы защиты информации компьютерной сети.

Система обнаружения атак (IDS – Intrusion Detection System) – это комплекс технических и программных средств, предназначенных для автоматизации процесса сбора и мониторинга событий, происходящих в компьютерной системе или сети, и дальнейшего анализа этих событий с целью выявления признаков нарушения безопасности объекта мониторинга.

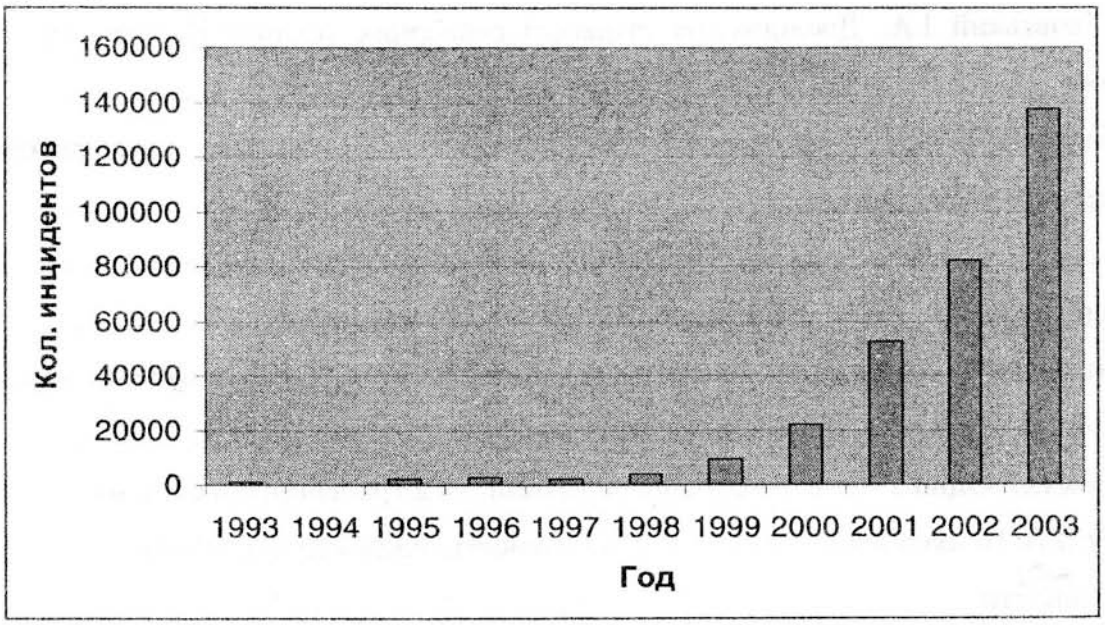


Рис. 1 Изменение количества инцидентов, связанных с нарушением безопасности, которые зарегистрированы в сети Internet за последнее десятилетие (согласно данным координационного центра CERT/CC)

Системы обнаружения атак используются с различными целями, среди которых можно выделить две основные:

а) с целью получения достаточного количества данных для расследования факта совершения атаки и выявления злоумышленника;

б) с целью повышения защищенности объекта защиты путем быстрого реагирования на обнаруженную атаку и устранения как самой атаки, так и ее последствий.

Кроме этого системы обнаружения атак могут быть использованы с другими целями, например:

– для выявления и устранения уязвимостей объекта защиты;
– для предотвращения атак, так как использование IDS увеличивает риск для атакующего быть обнаруженным;
– для оценки существующих угроз;
– для контроля качества администрирования созданной политики безопасности.

В настоящее время существует ряд систем обнаружения атак [2], которые используют различные методы мониторинга и анализа событий.

Основным достоинством метода обнаружения аномалий является возможность определения неизвестных атак. Однако системы, использующие этот метод, характеризуются высоким показателем ложных срабатываний.

Таким образом, метод обнаружения аномалий пока не может быть использован как основной метод обнаружения атак, но элементы обнаружения аномалий могут быть использованы совместно с методом обнаружения злоупотреблений, улучшая характеристики системы обнаружения атак.

Методы реагирования на обнаруженную атаку. Реакция на атаку выражается в действиях, направленных на защиту и (или) восстановление нормальной работы защищаемого объекта после обнаружения атаки. Выделяют активные и пассивные методы реагирования. При активном реагировании действия выполняются самой IDS, в то время как при пассивном реагировании выполнение действий возложено на человека, а система лишь сообщает об обнаружении атаки.

К группе активных методов относятся:

– сбор дополнительной информации о подозрительном событии (например, если сетевая IDS собирала пакеты, передаваемые только определенному IP-адресу или порту, то при обнаружении подозрительного события она может перейти в режим сбора всех пакетов);

– изменение окружающей среды (например, изменение настроек брандмауэра так, чтобы доступ в сеть пакетов с определенным IP-адресом источника был блокирован) с целью прекратить атаку, как только она была обнаружена;

– контратака.

К группе пассивных методов относится генерация сигналов и уведомлений с целью информировать пользователя об обнаружении атаки. Наиболее распространенный способ информировать пользователя о наступлении какого-либо события – это показать диалоговое окно на экране компьютера с информацией о событии. Информация может быть самой разнообразной: от простого уведомления о том, что атака произошла, до детального описания вида обнаруженной атаки, ее характеристик, инструментальных средств, с помощью которых эта атака была совершена, а также возможных последствий атаки. Сообщения также могут быть переданы удаленно с помощью компьютерной сети или посредством других средств связи, например, мобильной или пейджинговой. Основным недостатком удаленной передачи информации является повышение ее уязвимости. Поэтому использование альтернативных средств связи повышает надежность передачи. Также при передаче информации может быть использовано шифрование.

Заключение

Представленная базовая структура показывает состав и взаимодействие функциональных компонентов системы обнаружения атак. Приведенная классификация позволяет проанализировать методы обнаружения атак и сделать следующие выводы:

– распределенные системы обнаружения атак в общем случае имеют лучшие характеристики в сравнении с монолитными системами;

– несмотря на то, что требования, предъявляемые к мониторинговым и блокирующим IDS, являются противоположными, эти функции могут быть реализованы в одной системе обнаружения атак при условии, что такая IDS будет иметь два режима работы – мониторинговый и блокирующий;

– системы обнаружения атак, работающие в непрерывном режиме, в общем случае имеют лучшие характеристики в сравнении с системами, работающими в пакетном режиме;

– интеграция методов обнаружения атак на уровне сети, на уровне хоста и на уровне приложений в одной системе обнаружения, а также совместное использование методов обнаружения аномалий и методов обнаружения злоупотреблений улучшает характеристики IDS;

– система обнаружения атак должна использовать как активные, так и пассивные методы реагирования, но выбор используемого метода зависит от целей использования системы и принятой политики безопасности.

Работоспособность системы обнаружения атак можно оценить по таким показателям, как: точность обнаружения, своевременность обнаружения, количество обнаруживаемых атак, отказоустойчивость. Показателем точности обнаружения атак является количество ложных срабатываний (false alarms) системы обнаружения. Чем меньше этот показатель, тем эффективнее работает система. Своевременное обнаружение атаки дает возможность своевременно отреагировать на нее. Количество обнаруживаемых атак характеризует способность системы обнаруживать все атаки или только некоторое их подмножество. Чем выше этот показатель, тем эффективнее работает система. Сама IDS должна быть защищена от атак, а также иметь низкий показатель ошибок и сбоев в работе.

Системы обнаружения атак можно классифицировать по разным критериям (рис. 3).

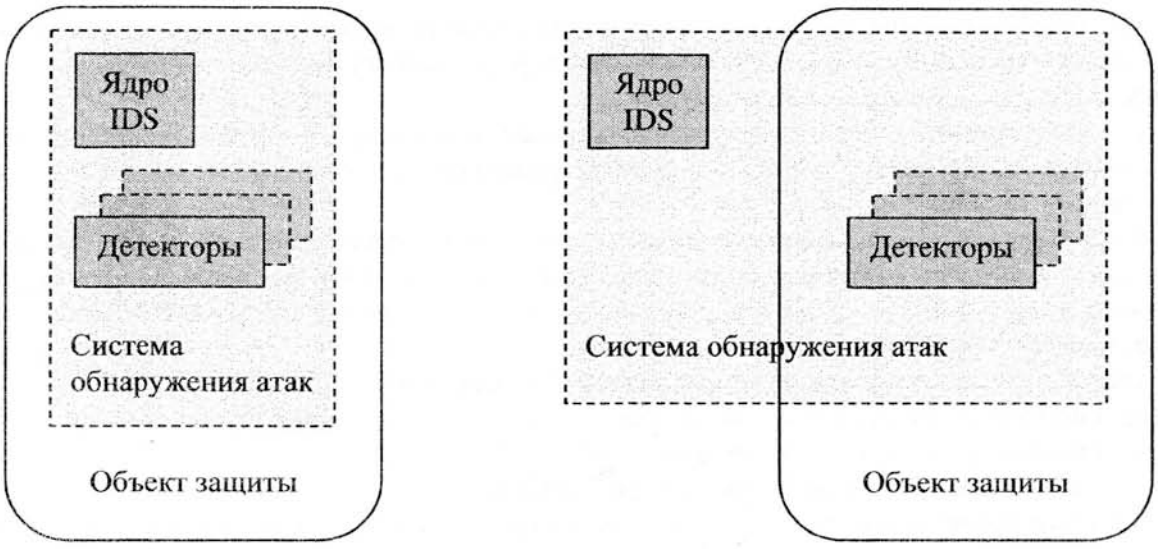
Рис. 3 Классификация систем обнаружения атак

Архитектура. Система обнаружения атак непосредственно взаимодействует, как минимум, с двумя системами – хостом и объектом защиты. На базе хоста работает ядро IDS (например, подсистема анализа данных, интерфейс взаимодействия с пользователем,

подсистема реагирования). На объекте защиты расположены детекторы IDS. Возможны два способа расположения хоста и объекта защиты:

а) в пределах одной компьютерной системы (рис. 4 а),

б) раздельно (рис. 4 б).



а) б)

Рис. 4 – Расположение IDS относительно других систем (а) в пределах одной компьютерной системы, б) раздельно)

В первом случае все компоненты IDS расположены в пределах одной компьютерной системы, т. е. IDS имеет монолитную архитектуру. Во втором случае IDS имеет распределенную архитектуру.

Цели использования IDS. Функциональные требования, предъявляемые к IDS, зависят от целей ее использования. Так, для получения информации, достаточной для расследования факта совершения атаки и выявления злоумышленника, система обнаружения атак должна работать в режиме мониторинга (мониторинговая IDS) и, как правило, не выявлять себя до тех пор, пока вся необходимая информация не будет получена. Если же целью использования IDS является повышение защищенности объекта защиты, то нужно как можно быстрее ликвидировать атаку и вернуть объект защиты в нормальное состояние, не заботясь о том, сколько данных об атаке было получено. По такому принципу работают блокирующие IDS.

Несмотря на то, что требования, предъявляемые к мониторинговым и блокирующим IDS, являются противоположными, эти функции могут быть реализованы в одной системе обнаружения атак при условии, что такая IDS будет иметь два режима работы – мониторинговый и блокирующий.

Стратегия управления. Стратегия управления предписывает то, как будет происходить управление компонентами IDS. Выделяют три способа управления: централизованное, частично распределенное и полностью распределенное.

При централизованном управлении все процессы IDS (сбор данных, их анализ и реагирование на обнаруженную атаку) управляются из одного пункта управления. При частично распределенном управлении процессы сбора данных и обнаружения атак управляются из локального пункта управления, а процесс реагирования – из одного или нескольких центральных пунктов управления, которые, в свою очередь, могут быть связаны иерархически. В данном случае предполагается, что локальные пункты управления расположены в пределах локальной сети, а центральные пункты управления могут располагаться за ее пределами. При полностью распределенном управлении, IDS должна иметь архитектуру, основанную на агентах [6].

Временные соотношения между процессом сбора данных и их анализом. Среди систем обнаружения атак можно выделить два вида систем:

1) системы, работающие в реальном режиме времени (непрерывный режим);

2) системы, работающие с временным интервалом между сбором данных и их анализом (пакетный режим).

В первом случае анализ данных производится по мере поступления их от детекторов. Во втором случае данные накапливаются за некоторый промежуток времени (например, за сутки), а затем выполняется их анализ.

Системы, работающие в непрерывном режиме, в отличие от систем, работающих в пакетном режиме, позволяют реагировать на обнаруженную атаку в момент или сразу после ее проведения.

Источники данных. Наиболее распространенный способ классификации систем обнаружения атак – по источникам данных. Одни системы используют для обнаружения атаки сетевые пакеты, в то время как другие системы анализируют события, генерируемые операционной системой или прикладными программами.

Таким образом, по источникам данных можно выделить:

а) системы, работающие на уровне сети;

б) системы, работающие на уровне хоста;

в) системы, работающие на уровне приложений.

Системы обнаружения атак, работающие на уровне сети, захватывают и анализируют сетевые пакеты. Одна IDS, установленная в одном из сегментов сети, может контролировать сетевой трафик в пределах всего сегмента и, таким образом, охранять все хосты этого сегмента. Распределенная сетевая система обнаружения атак может контролировать компьютерную сеть с большим количеством хостов. Внедрение сетевой IDS не должно вызвать каких-либо существенных изменений в структуре сети и повлиять на ее работу.

При внедрении и использовании сетевых систем обнаружения атак могут возникнуть следующие трудности:

– сбор и анализ сетевых пакетов в сетях с интенсивным трафиком требует большого объема памяти и высокой производительности вычислительной машины и может не дать положительного результата при распознавании распределенных во времени атак;

– так как зашифрованная информация не может быть проанализирована, то шифрование данных, передаваемых по сети (например, при использовании Virtual Private Network), исключает использование сетевой IDS;

– использование коммутаторов в качестве коммуникационного оборудования ограничивает возможности или усложняет использование сетевой системы обнаружения атак.

Системы обнаружения атак, работающие на уровне хоста, анализируют информацию, собранную в пределах отдельной компьютерной системы, например, о системных событиях, о процессах, о поведении пользователя. Такой подход позволяет делать достаточно точные выводы о наличии атаки и сопровождать эти выводы поясняющей информацией, например, - о пользователе или процессе, вовлеченном в атаку. Распределенная система обнаружения атак, работающая на уровне хоста, позволяет отслеживать состояние многих хостов.

В сравнении с сетевыми системами обнаружения атак, системы обнаружения атак, работающие на уровне хоста, имеют следующие преимущества:

– возможность обнаружения атак, которые принципиально не могут быть обнаружены на уровне сети (например, атаки, действие которых не выявляется за пределами хоста);

– возможность достоверного обнаружения факта совершения атаки и устранение ее последствий (сетевые IDS часто могут обнаружить только признаки атаки, но не факт ее совершения).

Недостатками систем обнаружения атак, работающих на уровне хоста, являются:

– так как IDS расположена и работает на базе хоста, то атака, направленная на хост (например, DoS-атака), может вывести из строя саму IDS;

– так как IDS использует вычислительные ресурсы объекта своего мониторинга, то повышаются требования к его техническим характеристикам;

– IDS на уровне хоста не может обнаружить те атаки, которые можно определить на уровне сети (например, сетевое сканирование).

Системы обнаружения атак на уровне приложений являются подмножеством систем обнаружения атак, работающих на уровне хоста, и анализируют события, которые генерируют программы. Такие системы позволяют выполнять тщательный мониторинг взаимодействия пользователя и программы и, таким образом, выявлять неавторизованную деятельность конкретного пользователя. Системы обнаружения атак, работающие на уровне приложений, более уязвимы к атакам, чем системы обнаружения атак, работающие на уровне хоста.

Возможности каждого метода обнаружения атак (на уровне сети, хоста или приложения) в отдельности ограничены и не позволяют обнаруживать все виды атак. В то же время эти методы не являются взаимоисключающими, а скорее дополняют друг друга. Таким образом, наиболее эффективной системой обнаружения атак будет та, которая интегрирует методы обнаружения атак на уровне сети, на уровне хоста и на уровне приложений.

Методы анализа данных. Используются два основных метода анализа событий для определения атак: определение злоупотреблений (Misuse Detection) и определение аномалий (Anomaly Detection).[2] Первый подход основан на выявлении признаков известных недопустимых данных. В настоящее время этот метод используется практически во всех коммерческих системах. Второй подход основан на определении недопустимых отклонений от нормального поведения объекта. Этот метод был и остается предметом дальнейших исследований.

Системы обнаружения атак, использующие метод определения злоупотреблений, анализируют деятельность объекта, просматривая события или последовательности событий и сравнивая их с предопределенными образцами известных атак. Такие образцы называют сигнатурами (signatures), а сам метод иногда называют методом определения атак на основе сигнатур (Signature-Based Detection). Соответствие сигнатуры некоторому событию (или последовательности событий) указывает на наличие атаки.

Определение злоупотреблений позволяет:

– достаточно эффективно обнаруживать известные атаки при низком показателе ложных срабатываний;

– быстро и достоверно определять инструментальные средства и приемы, используемые атакующим для реализации атаки.

В то же время анализаторы, работающие по принципу определения злоупотреблений, не способны выявить ту атаку, для которой нет образца. Это может быть либо неизвестная до сих пор атака, либо известная атака, которая выполнена необычно и, следовательно, не соответствует своему образцу. В любом случае система обнаружения атак, использующая метод обнаружения, основанный на сигнатурах, требует периодического обновления базы сигнатур.

Системы обнаружения атак, использующие метод определения аномалий, анализируют деятельность объекта на уровне сети, хоста или приложения с целью выявить его ненормальное (аномальное) поведение. Работа анализаторов по методу определения аномалий базируется на допущении, что признаком атаки служит некоторое отклонение от нормального поведения объекта. Сначала анализаторы создают профили нормального поведения пользователей, хостов и сетевых соединений на основе данных, собранных при нормальной работе объекта мониторинга. Затем текущие данные сравниваются с этими профилями для определения отклонений.

---

[2] Мы используем наиболее часто встречающиеся названия этих методов, хотя они могут называться по-другому. Например, в [6] эти методы названы Knowledge-based и Behavior-based, соответственно.

В базовый состав системы обнаружения атак обычно входят следующие компоненты (рис. 2): подсистема сбора данных, подсистема анализа данных, интерфейс взаимодействия с пользователем, база конфигурационных данных, база данных аудита.

Ряд авторов ([1, с. 10]) отмечают интеграцию систем обнаружения атак и систем реакции на атаку (Response System)[1], в то время как другие ([3, с. 8, 4, с. 6, 5, с. 2]) уже без всяких оговорок включают подсистему реагирования в состав основных функциональных компонентов IDS.

Детекторы предназначены для сбора данных, которые могут содержать информацию об атаках. Данные могут быть получены от любой части защищаемой системы (сети, хоста или приложения). На вход детекторов могут поступать, например, сетевые пакеты или файлы регистрации системных событий. Собранные данные затем передаются анализаторам.

Рис. 2 Базовая структура системы обнаружения атак

Анализаторы получают данные от одного или нескольких детекторов или от других анализаторов и предназначены для выявления признаков атаки. Выходной информацией анализатора является указание на наличие атаки. Эта информация может быть дополнена доказательством, подтверждающим выводы анализатора, а также описанием возможных последствий атаки. Выходные данные анализаторов сохраняются в базе данных аудита.

Интерфейс взаимодействия с пользователем позволяет просмотреть выходную информацию системы и дает возможность управлять системой при помощи консоли управления.

Подсистема реагирования предназначена для принятия решения о дальнейших действиях, направленных на восстановление нормальных условий функционирования объекта защиты, и выполнения этих действий после обнаружения атаки. На принятие решения влияют данные об обнаруженной атаке и конфигурационные данные системы.

В дополнение к указанным компонентам система обнаружения атак может включать такие компоненты как система выявления уязвимостей (Vulnerability Analysis System), средство проверки целостности файлов (File Integrity Checker), обманные системы (Honey Pot и Padded Cell).

Список литературы

1. State of the Practice of Intrusion Detection Technologies. J. Allen, A. Christie, W. Fithen, J. McHugh, J. Pickel, and E. Stoner. CMU/SEI Technical Report (CMU/SEI-99-TR-028), 2000. <URL: http://www.cc.gatech.edu/~wenke/ids-readings/ids-state.pdf>.
2. Sobirey, Michael. Michael Sobirey's ID Systems Page, 2000. <URL: http://www-rnks.informatik.tu-cottbus.de/~sobirey/ids.html>.
3. Becky Base and Peter Mell, Intrusion Detection Systems, National Institute of Standards and Technology Special Publication 800-31, 2001. <URL: http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf>.
4. Research in Intrusion Detection Systems: A Survey. S. Axelsson. Technical Report, 1999. <URL: http://www.cc.gatech.edu/~wenke/ids-readings/ids_research_survey.ps.gz>.
5. A Revised Taxonomy for Intrusion-Detection Systems. H. Debar, M. Dacier, and A. Wepsi. IBM Research Report, 1999. <URL: http://www.cc.gatech.edu/~wenke/ids-readings/IDS_taxonomy.ps>.
6. Balasubramaniyan, Jai, et al. (Purdue University). An Architecture for Intrusion Detection Using Autonomous Agents (Coast TR 98-05). West Lafayette, IN: COAST Laboratory, Purdue University, 1998. <URL: http:/ /www.cs.purdue.edu/coast/projects/autonomous-agents.html>.

Поступила 17.05.2004

УДК 65.012.8:354.31(477)

В.О. Хорошко, В.А. Кудінов

МЕТОДИЧНИЙ ПІДХІД ДО ФОРМАЛІЗАЦІЇ ЗАДАЧІ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОВС УКРАЇНИ

Вступ

Інформаційну систему (ІС) органів внутрішніх справ (ОВС) України розглядають як систему інформаційного забезпечення ОВС – це сукупність інформаційних автоматизованих підсистем певних обліків, призначених для збирання, накопичення, зберігання, обробки та використання інформації в діяльності підрозділів та служб ОВС України [1]. Вона здійснює всебічну інформаційну підтримку їх практичної діяльності у розкритті, розслідуванні та попередженні злочинів, встановленні і розшуку злочинців, надає багатоцільову статистичну, аналітичну та довідкову інформацію.

Подальший розвиток системи інформаційного забезпечення ОВС передбачений Програмою інформатизації органів внутрішніх справ України на 2000-2005 роки [2], яка містить розділ "Розробка та впровадження стратегії захисту інформації в інформаційній мережі ОВС України". У пункті 1 цього розділу передбачено: "Розробити концепцію комплексного захисту інформаційної системи ОВС України з метою забезпечення обробки конфіденційної інформації в інформаційних підсистемах ОВС України". У зв'язку з необхідністю виконання цього завдання дослідження проблеми оцінювання ефективності системи захисту інформаційної системи ОВС України є дуже актуальною проблемою.

Крім цього, робота відповідає тематиці приоритетних напрямів фундаментальних та прикладних досліджень вищих навчальних закладів та науково-дослідних установ МВС України на період 2002-2005 роки, яка затверджена наказом МВС України від 30 червня 2002 року № 635 [3]. Зокрема, у додатку 2 до наказу визначений такий напрям наукового дослідження: "Проблеми захисту інформації обмеженого користування в діяльності ОВС" (розділ 2, п.2.4).

Загальне дослідження стійкості багаторубіжної комплексної системи технічного захисту інформації проти дій зловмисника й ефективності розподілу її ресурсів між