УДК 681.3

Шорошев В.В., Хорошко В.А.

СИСТЕМЫ ОБНАРУЖЕНИЯ АТАК НА КОМПЬЮТЕРНЫЕ СИСТЕМЫ

Вопрос об актуальности и перспективности нового метода (технологии) защиты информационных ресурсов компьютерных систем от атак несанкционированного доступа (атак НСД) ранее уже поднимался [1-3]. Для фундаментального ознакомления с новой технологией информационной безопасности компьютерных систем путем обнаружения атак на их ресурсы рекомендуются работы [4-8]. Эта новая технология основана на мониторинге и нейтрализации любых атак, в том числе и атак НСД, к ресурсам компьютерных систем (КС), особенно наиболее распространенной их разновидности в виде Intranet, и обеспечивает реализацию политики их адаптивной безопасности путем создания и использования специальных систем обнаружения атак (System of detection of attacks или SDA-систем). В ведущих западных странах они получают все большее развитие. Работы по созданию SDA-систем ведутся также в России и на Украине. Поэтому уместно обратиться вначале к самой истории создания систем обнаружения атак.

В 1980 Джеймс Андерсон был первым, кто предложил использовать журналы регистрации в целях обеспечения информационной безопасности. Его концепция "Reference Monitor" была применена в ВВС США [4]. Это было рождение системы обнаружения атак, т.е. SDA-системы.

В 1984—1986 гг. Дороти Деннинг и Питер Ньюманн разработали абстрактную модель системы обнаружения атак в реальном масштабе времени, которая получила название IDES (Intrusion Detection Expert System — экспертная система обнаружения атак). В 1987 году Дороти Деннинг опубликовала документ, описывающий применение систем обнаружения атак для защиты информации. Данные исследования, как и многие другие, проводились в лабораториях Министерства обороны США. Система IDES базировалась на профилях и реализовала различные статистические методы, позволяющие описать нормальное и аномальное поведение субъектов системы, в основном, пользователей. Функционировала система IDES на компьютерах TOPS-20. В 1992—1994 гг. в лаборатории SRI International была разработана улучшенная версия этой системы — NIDES (Next-generation IDES — система IDES следующего поколения).

В 1986 году на базе IBM 3090 и языка COBOL была создана экспертная система Discovery для обнаружения проблем в финансовой базе данных TRW. Целью разработки Discovery был контроль ежедневных финансовых транзакций и поиск в них несанкционированных платежей. Собственно, эта система скорее относится к классу систем обнаружения мошенничества, нежели чем к обнаружению атак.

В 1988 году по заказу U.S. Air Force Cryptologic Support Center была претворена в жизнь система обнаружения аномального поведения Haystack. Начало данной системе было положено компанией Tracer Applied Sciences, Inc. (1987—1989), а затем разработка перешла в ведение Haystack Labs (1989— 1991), только потом в Trusted Information Systems и Network Associates. Система Haystack была разработана для платформы IBM AT с использованием стандарта ANSI языка C и базы данных Oracle. Эта система была одной из первых ориентированных на персональные компьютеры.

Система MIDAS (Multics Intrusion Detection and Alerting System) была разработана в 1988 году специалистами National Computer Security Center (NCSC) для обнаружения аномалий в сети Dockmaster этого центра, функционирующей под управлением ОС Multics на платформе Honeywell DPS 8/70. Как и все предыдущие системы, MIDAS использовала в своей работе статистические методы, позволяющие зафиксировать аномальное поведение субъектов системы на основе записей журналов регистрации. MIDAS была первой SDA-системой, которая контролировала узлы, подключенные к сети Internet, и тем самым могла распознавать внешние по отношению к NCSC атаки. В 1990 году в национальной

лаборатории Лос-Аламоса была создана система NADIR (Network Audit Director and Intrusion Reporter) для контроля деятельности пользователей, подключенных к сети ICN (Integrated Computing Network). Система запускалась на хостах с операционной системой Sun Unix и использовала в своей работе СУБД Sybase. Это одно из немногих средств обнаружения атак, разработанных в конце 80-х — начале 90-х годов, которое работает до сих пор.

Новая концепция систем обнаружения атак была представлена в 1990 году вместе с появлением системы NSM (Network Security Monitor, сейчас называемой Network Intrusion Detector, NID) [5]. Эта концепция вместо исследования журналов регистрации предлагала анализ сетевого трафика для обнаружения атак несанкционированной деятельности (атак НСД). Система NSM вышла из стен университета Дэвиса в Калифорнии (UC Davis) и функционировала на рабочих станциях Sun Unix.

В 1991 появляется DIDS (Distributed Intrusion Detection System) — система, позволяющая получать данные от нескольких систем обнаружения атак для выявления скоординированных атак сразу на несколько узлов сети. Основное достоинство DIDS заключалось в том, что она позволяла одновременно получать данные как от агентов, контролирующих системные журналы регистрации, так и от агентов, фиксирующих сетевой трафик. Исследования данной возможности велись по заказу ВВС США, Агентства Национальной Безопасности США (National Security Agency) и Министерства Энергетики США в U.S. Air Force Cryptologic Support Center, национальной лаборатории Lawrence Livermore, университете Дэвиса и лаборатории Haystack.

В 1994 году Марк Кросби и Юджин Спаффорд предложили идею автономных агентов [9], позволяющих улучшить такие характеристики систем обнаружения атак, как масштабируемость, эффективность, отказоустойчивость.

Другой подход, облегчающий масштабирование системы обнаружения атак, нашел применение в 1996 году в системе GrIDS (Graph-based Intrusion Detection System). Эта система сводит к более простым действиям обнаружение крупномасштабных и скоординированных атак [8]. Как и многие другие названные системы обнаружения атак, GrIDS была разработана в университете Дэвиса.

В конце 90-х годов образовались новые подходы к обнаружению атак, отличающиеся от классических. К таким подходам можно отнести применение генетических алгоритмов [8] и нейронных сетей для обнаружения нарушений политики безопасности. Эти подходы фактически уже вышли за рамки научно-исследовательских работ. Например, работы Джеймса Кеннеди в области применения нейронных сетей [6] позволили существенно увеличить вероятность обнаружения неизвестных атак в SDA-системе RealSecure.

Данные примеры являются основополагающими в области обнаружения атак. Именно упомянутые средства, разработанные в рамках НИОКР, послужили прототипами широко известных в настоящее время коммерческих систем обнаружения атак, таких как RealSecure, Cisco Secure IDS и др. Далее рассмотрим классификацию и базовый состав наиболее популярных SDA-систем согласно модели политики мониторинга нарушений политики безопасности КС (рис.1).

Классификация и состав систем обнаружения атак НСД

В работах [1-3] уже освещались недостатки традиционных методов защиты ресурсов корпоративных сетей Intranet (межсетевые экраны, фильтрующие маршрутизаторы, пакеты фильтрующих программ, системы обнаружения атак и др.).В работе [3] рассмотрены два варианта классификации и базового состава SDA-системы для обнаружения атак НСД. В

развитие изложенного подхода в [1-3] предлагается перейти к использованию нового мониторинго - адаптивного метода защиты путем обнаружения атак НСД (monitoring-adaptive method of protection by detection of attacks, MamPda-метод) как дополнения к традиционным методам защиты.

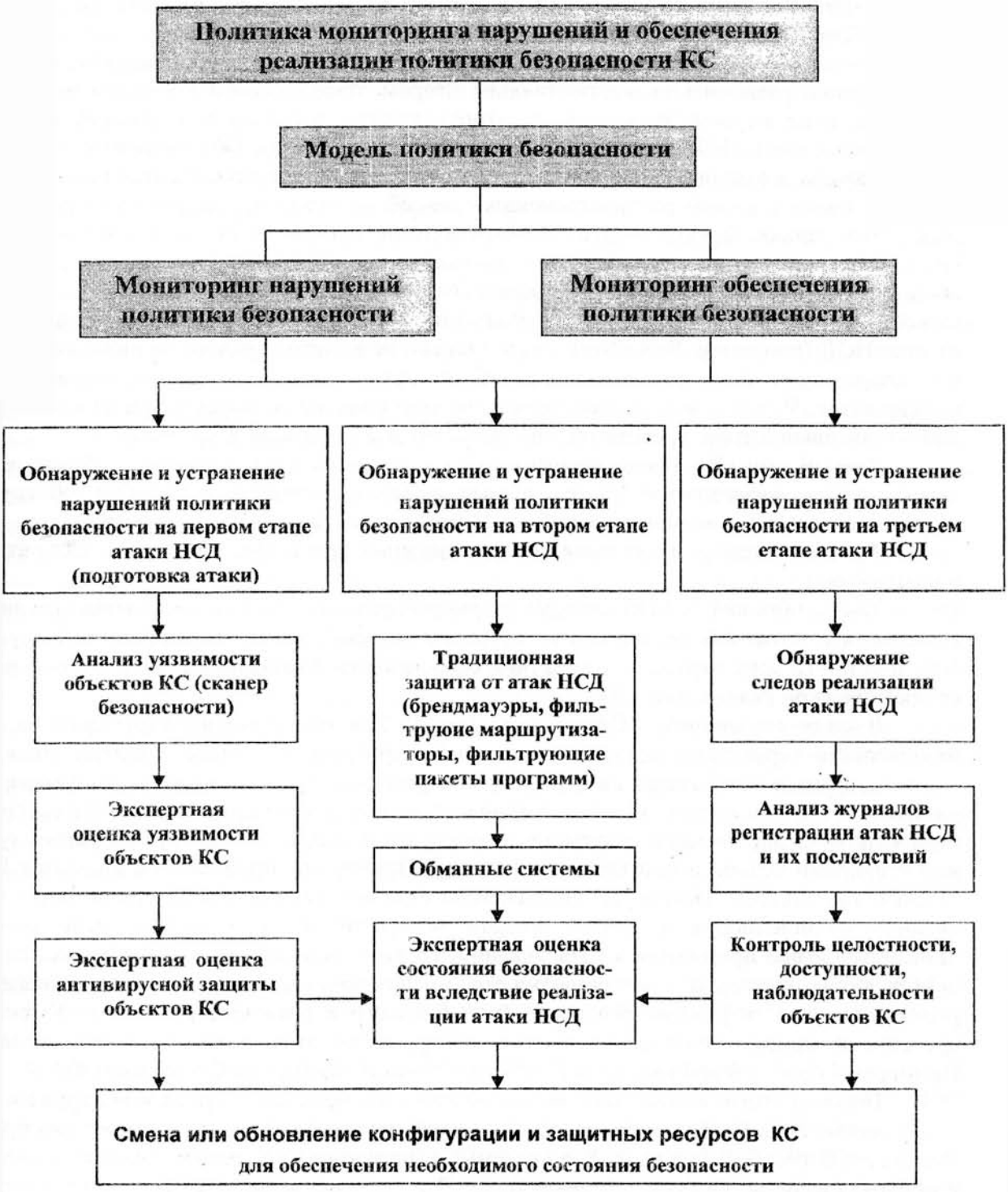

Рис. 1. Модель политики мониторинга нарушений политики безопасности КС и обеспечения ее реализации

Суть предложенного метода защиты можно сформулировать следующим концептуальным правилом адаптивной безопасности MamPda-1: если мы не можем построить абсолютно защищенную компьютерную систему от атак НСД, то хотя бы должны обнаруживать все (или практически все) нарушения политики безопасности и соответствующим образом (адаптивно) реагировать на них.

Практически это возможно только путем своевременного обнаружения атаки НСД (первый этап защиты от нее), а также ее нейтрализации при попытке реализации (второй этап защиты). Технология атак НСД имеет еще и третий этап их реализации – заметание следов (завершение атаки, скрытие источника и факта атаки НСД), поэтому обнаружение атаки на третьем этапе равносильно поражению, на втором этапе – почти успешная зашита, но с потерями, а на первом этапе – почти 100% защиты ресурсов КС, Intranet, если после обнаружения атаки НСД вы можете ее на 100% нейтрализовать. Обнаруживать, блокировать и предотвращать нарушения политики безопасности КС можно несколькими способами.

Первый и самый распространенный способ — это распознавание уже реализуемых атак. Этот способ функционирует на втором этапе защиты от атаки, в том числе и атаки НСД, т.е. при ее реализации. Этот способ применяется в "классических" системах обнаружения атак (например, RealSecure Network Sensor или Cisco IDS), а также в межсетевых экранах (таких как Check Point Firewall-1 и др.), системах защиты информации от атак НСД (например, SecretNet) и т. п. Однако недостаток средств данного класса в том, что атаки могут быть реализованы повторно. Они также повторно обнаруживаются и блокируются. И так далее, до бесконечности, что конечно неэффективно, т. к. приводит к непозволительной трате временных, человеческих и материальных ресурсов.

Второй способ - предотвращение атак еще до их осуществления. Реализуется он путем поиска уязвимостей (т. е., иными словами, представляет собой обнаружение потенциальных атак), которые могут быть использованы для совершения атаки.

Третий способ — выявление уже совершенных атак и предотвращение их повторения в дальнейшем.

Таким образом, в SDA-системе (априори принимается к обязательной) реализуется концепция адаптивной безопасности, в основе которой лежит мониторинг (обнаружение) всех или почти всех нарушений политики безопасности и мониторинг степени обеспечения ее практической реализации в КС.

В силу сказанного, SDA-системы (рис.1) для обнаружения нарушений политики безопасности структурно могут быть классифицированы по этапам развития атаки НСД: системы, функционирующие на первом этапе развития атаки и позволяющие обнаружить уязвимости КС или корпоративной сети Intranet, используемые нарушителем. Иначе средства этой категории называются системами анализа защищенности (security assessment systems) или сканерами безопасности (security scanners). Примерами таких систем являются Internet Scanner или SATAN. Некоторые специалисты считают неправильным причисление систем анализа защищенности к классу средств обнаружения атак, однако, если следовать описанным выше принципам классификации, то такое отнесение вполне логично; системы, действующие на втором этапе развития атаки и позволяющие выявить атаки в процессе их реализации, т. е. в режиме реального (или близкого к реальному) времени. Именно эти средства и принято считать системами обнаружения атак в классическом понимании. Примерами таких систем являются RealSecure Network Sensor или OkenaStormWatch.

Помимо этого, в последнее время выделился новый класс средств обнаружения атак — обманные системы (deception systems). В качестве примера таких систем можно привести RealSecure Server Sensor или DTK и системы, действующие на третьем этапе развития атаки и обнаруживающие уже совершенные атаки. Эти системы делятся на два класса — системы контроля целостности (integrity checkers), отслеживающие изменения контролируемых ресурсов, и системы анализа журналов регистрации (log checkers). В качестве примеров таких систем могут быть названы Tripwire или RealSecure Server Sensor.

Помимо приведенной, существует еще одна распространенная классификация систем обнаружения нарушения политики безопасности — по уровню реализации атаки НСД: host-based - системы, т. е. обнаружение уязвимостей или атак, направленных на конкретный узел сети Intranet; network-based – системы, т. е. обнаружение уязвимостей или атак, направленных на всю сеть или сегмент сети Intranet.

Классификация систем обнаружения атак по этапам их реализации, представленная на рис. 1, и ее дальнейшая детализация на этом обычно останавливается. Однако, основываясь на классификации уровней КС, например, корпоративной сети Intranet, сетей Netware [3,8], можно выделить еще три подуровня: системы обнаружения атак на уровне прикладного ПО (application-based), выявляющие атаки на конкретные приложения (например, на Web-сервер). Примерами таких систем являются RealSecure OS Sensor или WebStalker Pro; системы обнаружения атак на уровне ОС (OS-based), распознающие атаки на уровне операционной системы. Примерами таких систем служат DirectoryAlert и ServerAlert компании NetVision, обнаруживающие атаки в сетях Netware; системы обнаружения атак на уровне системы управления базами данных (DBMS-based), обнаруживающие атаки на конкретные системы управления базами данных (СУБД).

Выделение средств обнаружения атак на СУБД в отдельную категорию связано с тем, что современные СУБД уже вышли из разряда обычных прикладных приложений и по многим своим характеристикам, в т. ч. и по сложности, приближаются к операционным системам. При этом системы обнаружения атак (точнее, системы анализа защищенности) на уровне СУБД могут функционировать как на самом узле, так и через сеть (например, Database Scanner). В свою очередь, система обнаружения атак на уровне сети может быть локализована и на конкретном узле для регистрации атак, направленных не на все узлы сегмента, а только на тот, на котором она установлена. Пример такой системы — RealSecure Desktop Protector. Сразу надо отметить, что данная классификация может вызвать споры. Многие специалисты считают неправильным отнесение сканеров безопасности к системам обнаружения атак. Аналогичная ситуация и с системами контроля целостности и анализа журналов регистрации. Эти системы помогают в обнаружении атак, "но на системы IDS совсем не похожи" [6]. Не будем оспаривать этот факт, заметим только, что, учитывая этапы реализации атак, приведенная классификация вполне закономерна.

Кроме того, до сих пор не выработана единая терминология в этой области. Каждый производитель, желая показать, что его система уникальная и превосходит другие решения, создает новый класс систем обнаружения атак. Так появились гибридные системы обнаружения атак (например, Prelude IDS), виртуальные системы обнаружения атак (например, IntruShield от In-truVert), многоуровневые системы (multitiered IDS), шлюзовые (gateway IDS), системы с контролем состояния (stateful IDS) и даже системы, основанные на спецификациях (specification-based IDS) или стеке (stack-based IDS) и т. д.

Выводы

Рассмотренные образцы популярных зарубежных систем обнаружения атак, их классификация и типовой состав на примере базовой модели мониторинга нарушений и обеспечения политики безопасности КС позволяют сделать следующие выводы и рекомендации.

Во-первых, обзор популярных зарубежных систем обнаружения атак поможет, на наш взгляд, специалистам оценить актуальность и необходимость приобретения зарубежных или создания отечественных перспективных систем обнаружения атак.

Во-вторых, предлагаемая модель мониторинга нарушений и обеспечения политики безопасности компьютерных систем и сетей Интранет поможет, на наш взгляд, специалистам выработать наиболее обоснованные требования к содержанию, формулированию и реализации перспективной политики их адаптивной безопасности.

В-третьих, первоочередными требованиями к политике адаптивной безопасности любой SDA-системы в любой ее конфигурации следует считать:

- обнаружение любой атаки на ее первом этапе, т.е. при изучении объектов атаки, и прежде всего, объектов сети Интранет;
- анализ уязвимости объектов КС с помощью сканеров безопасности и устранение выявленных нарушений политики безопасности;
- анализ журналов регистрации атак НСД и их последствий;

- контроль целостности, доступности и наблюдательности объектов защиты КС;
- експертная оценка информационной и антивирусной безопасности объектов защиты КС для оценки их соответствия заданным требованиям.

Наконец, выполнение предложенных рекомендаций носит не только теоретический характер (методологический, методический, концептуальный, отечественно приоритетный) , но и практический. Это обусловлено тем, что все существующие технологии защиты безопасности компьютерных систем и сетей не стопрцентны по надежности и это вполне закономерно, так как абсолютно надежной защиты КС не существует вообще, поскольку ситуация безопасности носит всегда дуэльный характер по общеизвестному принципу противоборства интересов: с одной стороны - пользователя КС и с другой стороны – нарушителей реализации или соблюдения их интересов.

Кроме того, дело в том, что любая защита не может быть универсальной вообще, она всегда конкретна под определенные угрозы, для конкретных объектов КС, под конкретную конфигурацию КС, под конкретно выбранную политику безопасности КС, при использовании конкретных функциональных (услуги К,Ц,Д,Н) и гарантийных (Г-1…Г-7) услуг безопасности, а также при конкретной степени их реализации по критерию «вид информационной деятельности с использованием КС-эффективность безопасности - гарантия безопасности - стоимость безопасности» и др.

Список литературы

1. *Шорошев В.В.* Недостатки традиционных средств защиты корпоративных сетей Интранет и необходимость применения новых методов их защиты. Бизнес и безопасность № 2, 2003, с.54-59;

2. *Шорошев В.В.* Перспективный метод защиты инормационных ресурсов корпоративных сетей Интранет. Бизнес и безопасность № 6, 2003, с38-46;

3. *В.Шорошев.* Перспективный метод защиты инормационных ресурсов корпоративных сетей Интранет. Науково-технічний збірник НТУ «КПІ» № 7, 2003. С.62-77;

4. *Rebecca Gurley Bace*. Intrusion Detection. Macmillan Technical Publishing, 2000;

5. *Panagiotis A* stithas. Intrsion Detection Systems. 1999;

6. [Cannadyl-98] James Cannady. Atificial Neural Networks for Misuse Detection. 1998;

7. *Грег Шипли.* Оружие компьютерного подполья. Сети и ситемы связи, № 10, 2000;

8. *Лукацкий А.В.* Обнаружение атак. – 2-е изд., перераб. и доп. - СПб.: БХВ-Петербург, 2003. – 608 с.: ил.

УДК 004.056.5

Васильцов І.В., Дубчак Л.О.

КЛАСИФІКАЦІЯ СУЧАСНИХ АТАК СПЕЦІАЛЬНОГО ВИДУ НА РЕАЛІЗАЦІЮ

Вступ

Задача захисту інформаційних ресурсів постає особливо гостро в умовах розвитку сучасних інформаційних технологій. Постійне зростання об'ємів інформаційних ресурсів обумовлює жорсткі вимоги до засобів шифрування/дешифрування стосовно швидкості опрацювання вхідних даних. Природно, що для вирішення цієї задачі необхідно використовувати апаратну реалізацію відомих алгоритмів криптографічного захисту інформації [1-3, 4-5].

Проте такі тенденції до апаратної реалізації засобів криптографічного захисту інформації в свою чергу обумовили появу принципово нових видів криптоаналізу, які умовно можна назвати "Атаки спеціальних впливів" або ж "Атаки на основі нестандартних