Системы обнаружения вторжений в комплексе информационной безопасности банков

Intrusion detection systems in the information security complex of banks

Бойченко / Boychenko O.
Олег Валериевич
(bolek61@mail.ru)
доктор технических наук, профессор,
член-корреспондент Российской Академии Естествознания.
ФГАОУ ВО «Крымский федеральный университет имени В. И. Вернадского»,
профессор кафедры бизнес-информатики и математического моделирования.
г. Симферополь

Гавриков / Gavrikov I.
Илья Владимирович
(painttool@gmail.com)
ФГАОУ ВО, ассистент кафедры бизнес-информатики и математического моделирования.
г. Симферополь

Ключевые слова: система обнаружения вторжений – intrusion detection system; классификация – classification; эффективность – efficiency; компьютерные сети – computer networks; сетевая безопасность – network security; машинное обучение – machine learning; искусственный интеллект – artificial intelligence.

В статье исследована роль систем обнаружения вторжений как составной части комплекса безопасности современного банка для защиты данных в информационных системах и информационных сетях. Рассмотрен общий принцип функционирования таких систем и их классификация по различным критериям и показателям, а также приведены преимущества и недостатки как экономические, так и технические (для различных классов систем обнаружения вторжений). В статье также приведены результаты экспериментального исследования функционирования системы обнаружения вторжений авторской разработки, основанной на технологиях машинного обучения, и предложены дальнейшие направления развития.

The article investigates the role of intrusion detection systems as an integral part of the security complex of a modern bank for data protection in information systems and information networks. The general principle of functioning of such systems and their classification as per various criteria and indicators is considered, and advantages and shortcomings both economic, and technical (for various classes of intrusion detection systems) are also given. The article also presents the results of an experimental study of the functioning of the intrusion detection system of the author's development based on machine learning technologies and proposes further development directions.

Потребность в надёжных средствах информационной безопасности сегодня растёт особенно быстрыми темпами. В последние годы значительно возросли количество и калибр кибератак – так, по данным опроса НАФИ от ноября 2017 г., российские компании потеряли из-за кибератак 115,97 млрд. рублей, а средний объём потерь одной компании за год составил около 300 000 рублей [1].

Вопрос обеспечения информационной безопасности особенно актуален в банковской сфере по двум основным причинам:

· атаки на информационные системы в финансовом секторе могут привести к крупным потерям, поскольку эти информационные системы обеспечивают передвижение крупных объёмов средств;

· банковские информационные системы нередко используют морально устаревшее программное и аппаратное обеспечение.

Так, по оценкам Международного валютного фонда [2], средние ежегодные потери от потенциальных атак на финансовую систему могут привести к потере около 9% глобальной прибыли всей банковской системы, а в худшем сценарии эти потери могут приблизиться к 50% банковской прибыли.

Непосредственное воздействие на систему изнутри остаётся актуальным вектором атаки, и немалая доля средств защиты от таких атак представлена корректным планированием и внедрением информационной архитектуры, а также административными мерами. Однако атаки на информационные сети также представляют значительную опасность, и если в прошлом крупномасштабные атаки требовали ресурсов, доступных

только крупным организациям, сегодня эффективные атаки на крупные информационные системы могут быть проведены даже относительно немногочисленными хорошо организованными группами злоумышленников. В этих условиях организациям необходимы решения, способные надёжно защитить информационные сети от вторжений.

Целью данной работы является рассмотрение классов систем обнаружения вторжений, их экономических и технических преимуществ и недостатков, а также особенностей внедрения таких систем на практике.

Системы обнаружения вторжений (СОВ), также называемые IDS (intrusion detection system), представляют собой программные комплексы, сигнализирующие об обнаружении атак на компьютерную сеть, за которой ведётся наблюдение. Их целью является защита сети при помощи комбинирования сигнала, издаваемого при обнаружении атаки на неё, и комплекса мер, применяемых ответственным специалистом по безопасности для предотвращения нанесения урона системе злоумышленником. СОВ не решают сами по себе проблемы, связанные с безопасностью информационной системы или сети ИС, но сообщают о таких проблемах ответственным лицам для принятия ими необходимых решений и мер. Существуют различные классы СОВ, каждый из которых имеет сильные и слабые стороны в определённой сфере применения, и для различных классов СОВ различным образом распределяются средства на их установку и поддержку.

На самом макроскопическом уровне система обнаружения вторжений может быть описана как датчик, обрабатывающий информацию из системы, подлежащей защите (рис. 1). Такой датчик использует для работы информацию трёх видов: долгосрочную информацию для механизма обнаружения вторжений (например, база знаний атак), конфигурационную информацию о текущем состоянии системы, и информацию аудита, описывающую события в системе. Ролью датчика является исключение ненужной информации из аудита и синтетический обзор всех действий, предпринятых пользователями (ширина стрелки отображает объём информации, передаваемой между элементами.). После этого осуществляется оценка вероятности того, являются ли эти действия симптомами вторжения.

В качестве основных критериев оценки эффективности и адекватности СОВ можно выделить следующие:

· точность в данной работе определена как отношение количества событий в системе, классифицированных СОВ как легитимные, к истинному количеству легитимных событий;

· полнота определена как отношение количества событий в системе, классифицированных СОВ как злонамеренные, к истинному количеству злонамеренных событий. Этот критерий трудно оценить точно, поскольку в реальных условиях невозможно иметь абсолютное знание о всех видах атак;

· производительность СОВ можно определить как скорость обработки событий в аудите. Если СОВ характеризуется низкой производительностью, обнаружение вторжений в реальном времени становится невозможным;

· устойчивость – СОВ должна сама быть устойчива к атакам, в особенности атакам класса DoS, и должна разрабатываться с учётом этих требований. Это особенно важно, поскольку большинство СОВ работают на основе коммерческих операционных систем и аппаратного обеспечения, которые уязвимы для атак;

· своевременность СОВ определяется выполнением анализа и извещении о его результатах максимально быстро, так чтобы ответственное лицо могло среагировать на атаку, пока системе не был нанесён значительный урон и пока сам злоумышленник не сумел скомпрометировать источник данных аудита или саму СОВ. Данный критерий не является синонимом производительности, поскольку включает в себя также время, необходимое для реакции на атаку.

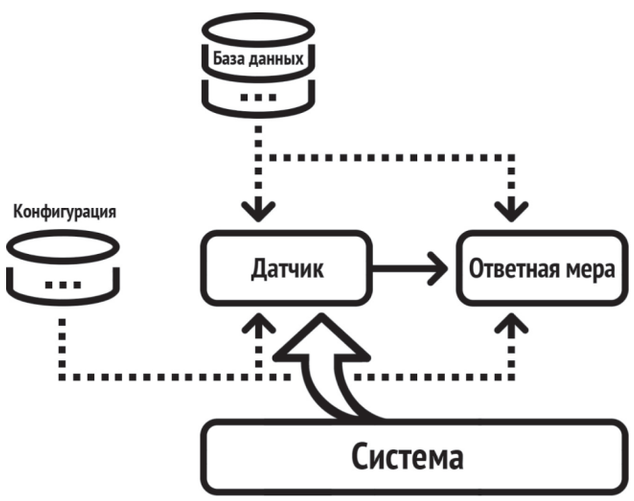

Рис. 1. Общая схема системы обнаружения вторжений [3]

Основным экономическим критерием оценки СОВ является её стоимость. Стоимость можно условно определить как объём средств и ресурсов, необходимых для поддержания всех вышеуказанных (технических) критериев на приемлемом уровне.

Классификацию систем обнаружения вторжений можно провести по ряду признаков и особенностей реализации:

1. Источник данных аудита описывает то, откуда СОВ берёт информацию, по которой проводится анализ. По источнику данных системы разделяются на следующие категории:

· системы обнаружения уровня сети (*network intrusion detection system, NIDS*), собирающие информацию об информационных потоках в ИС;

· системы обнаружения уровня хоста (*host intrusion detection system, HIDS*), собирающие информацию о событиях в наблюдаемой информационной системе.

2. Поведение при обнаружении описывает меры, предпринимаемые самой СОВ по обнаружению вторжения в систему. По поведению системы разделяют на пассивные, генерирующие только сигналы и сообщения об обнаруженных вторжениях, и активные, самостоятельно предпринимающие меры по предотвращению злонамеренных действий (закрытие портов, завершение сеансов злоумышленников и др.). В некоторых источниках СОВ называются только пассивные системы, а для активных определяется термин «система предотвращения вторжений» (i*ntrusion prevention system, IPS*) или «система обнаружения и предотвращения вторжений» (intrusion detection and prevention system, IDPS) [4].

3. Механизмы, при помощи которых СОВ осуществляют обнаружение вторжений в компьютерные сети, включают в себя:

· обнаружение злоупотреблений (*misuse detection*), или обнаружение на основе знаний – обнаруживает атаки на наблюдаемые системы, основываясь на базе (или базах) знаний уже известных атак;

· обнаружение аномалий (*anomaly detection*), или обнаружение на основе поведения – обнаруживает любые отклонения от нормальной работы систем, основываясь на профиле их нормальной работы.

СОВ, построенные на механизме обнаружения злоупотреблений (далее ЗСОВ), осуществляют поиск по базам известных шаблонов атак и злонамеренных действий. В таких СОВ всякое действие, не распознанное однозначно как атака, считается приемлемым. Благодаря этому ЗСОВ отличаются относительно высокой точностью, в особенности по отношению к широко известным видам атак, однако поддержание высокого уровня полноты системы требует регулярного обновления баз знаний атак. В качестве других преимуществ ЗСОВ можно выделить низкую частоту ложных тревог и высокий уровень детализации предложенного анализа, что упрощает процесс принятия превентивных или корректирующих мер ответственным лицом.

Основными недостатками подхода на основе знаний является трудоёмкость процесса сбора необходимой информации и её постоянного обновления для учёта новых сред и уязвимостей. Поддержка базы знаний СОВ требует детального анализа каждой уязвимости и поэтому требует значительных затрат со стороны предприятия, внедряющего СОВ в свой комплекс информационной безопасности. ЗСОВ также страдают от проблемы обобщения, поскольку большинство векторов атак используют уязвимости, тесно связанные с конкретными средами, условиями и конфигурациями, что обуславливает появление следующих проблем:

· ЗСОВ с низкой стоимостью способны обнаруживать только небольшую часть всех потенциальных вторжений в ИС предприятия;

· ЗСОВ, способные адекватно обнаруживать различные классы вторжений, имеют высокую стоимость.

ЗСОВ также испытывают значительные трудности с обнаружением инсайдерских атак со злонамеренным использованием привилегий, поскольку в таком сценарии злоумышленником не используются уязвимости как таковые.

С экономической точки зрения, применение ЗСОВ требует значительных вложений для обеспечения высокого уровня защиты, однако внедрение ЗСОВ с достаточно полным набором правил на практике гарантирует достаточный уровень защиты банковской информации. Таким образом, целесообразность использования ЗСОВ для предприятий (банков), нуждающихся в высоком уровне безопасности и располагающих достаточными ресурсами для его обеспечения, обусловлена гарантированно стабильным обнаружением вторжений, использующих известные векторы атаки. Однако для обеспечения защиты от новых векторов атаки предприятию необходим штат опытных ИБ-сотрудников.

Рассмотрим различные классы ЗСОВ.

1. Экспертные системы [5] характеризуются наборами правил, описывающих атаки. События аудита переводятся системой в факты с семантической значимостью в экспертной системе, а механизм логического вывода системы делает заключения на базе этих правил и фактов. Такой метод увеличивает уровень абстракции данных аудита. В моделировании знаний экспертов наиболее часто используются языки правил, что позволяет проводить систематический поиск признаков вторжения по данным аудита.

Однако использование языков правил имеет ряд ограничений:

· проблема создания знаний заключается в сложности выделения уникальных признаков атак и перевода их в правила с использованием данных аудита в качестве входа. Информация, требуемая для определения события как атаки, может не содержаться в данных аудита. Также на основании одной уязвимости зачастую существует множество векторов атак, каждый из которых требует создания собственного правила;

· проблема скорости обработки истекает из показателей производительности экспертных систем, которые

могут быть недостаточными для производительной и своевременной СОВ.

2. Сигнатурный анализ [6] повторяет принцип получения знаний экспертных систем, но отличие между этими двумя способами заключается в механизме использования этих знаний. В сигнатурном анализе семантическое описание атак переводится в правила, содержащие информацию, которая может быть непосредственно найдена в данных аудита. Исторически сигнатурами являлись последовательности байтов в сетевых пакетах, которые уникально идентифицировали вредоносные сетевые пакеты или коды для консольных оболочек. Сегодня правила, используемые в системах сигнатурного анализа, в дополнение к собственно сигнатурам могут также включать в себя ряд дополнительных признаков, таких как информацию о сетевом протоколе; информацию об источнике; информацию о приёмнике; направление передачи данных; порты; флаги протокола и др.

Во многих современных ЗСОВ между отдельными правилами также могут существовать логические связи, позволяющие создавать сложные составные правила для обнаружения комплексных атак. Это также позволяет снизить количество ложных срабатываний.

С использованием сигнатурного анализа также связана проблема создания знаний, в особенности аспект множественности правил: в ЗСОВ, работающей на ряде платформ, должны иметься правила обнаружения одного вида атак для каждой из платформ. Это значительно увеличивает объём ресурсов, затраченных на создание таких правил, и соответственно повышает стоимость такой СОВ.

3. Другим потенциальным методом описания шаблонов вторжений является использование различных сетей Петри [7]. Преимуществами сетей Петри являются их концептуальная простота, способность описания шаблонов в общем виде и возможность графического представления. Тем не менее их использование требует относительно высоких вычислительных мощностей, из-за чего они пока используются только в экспериментальных прототипах.

Противоположностью ЗСОВ являются СОВ, построенные на механизме обнаружения аномалий или отклонений от нормальной работы (далее АСОВ) [8]. В таких системах любое отклонение от установленного профиля нормального поведения в информационной системе распознаётся как внедрение. Этот профиль может генерироваться и храниться различными способами. Использование механизма обнаружения аномалий обеспечивает достаточно высокий показатель полноты, но достаточно сложным становится поддержание высокого уровня точности.

Одно из главных преимуществ АСОВ заключается в их способности обнаруживать новые, неизвестные ранее атаки – как новые подходы к использованию уже существующих уязвимостей, так и совершенно новые векторы атаки с использованием так называемых «уязвимостей нулевого дня». АСОВ также способны обнаруживать атаки типа «злоупотребление привилегиями», которые не используют уязвимости как таковые.

В качестве основного недостатка АСОВ чаще всего выделяют высокое количество ложных тревог, генерируемых такими системами [9]. Это обусловлено тем фактом, что в фазе обучения системы могут оказаться непокрытыми все возможные действия и всё возможное поведение пользователей. Помимо этого, поведение пользователей меняется со временем, что требует регулярного обновления профиля нормальной работы – это может на некоторое время вывести систему из строя или стать причиной дополнительных ложных тревог.

С экономической точки зрения, использование АСОВ в деятельности банков может послужить средством экономии ресурсов, поскольку для неё не требуется регулярно создавать наборы правил обнаружения вторжений, поскольку процесс обновления профиля нормальной работы системы не требует от ИТ-специалистов столь высоких затрат.

Рассмотрим основные классы АСОВ.

1. Стандартным подходом к реализации АСОВ является использование статистических методов. Поведение пользователей анализируется посредством оценки ряда переменных с течением времени. Такими переменными могут выступать время начала и завершения сессии, длительность доступа к ресурсам и другие. Временные отрезки могут продолжаться от нескольких минут до месяца. Модель содержит в себе средние значения отслеживаемых переменных и определяет превышение допустимых порогов, основываясь на стандартном отклонении. Однако такая модель относительно примитивна и недостаточно точно определяет атаки.

2. По аналогии с ЗСОВ, экспертные системы могут использоваться и для АСОВ, конструируя правила, отвечающие нормальному поведению пользователей в системе. Тем не менее экспертные системы остаются относительно низкопроизводительным подходом и менее эффективны в условиях обработки больших объёмов данных.

3. Машинное обучение представляет собой использование различных алгоритмов, которые обрабатывают информацию, динамически изменяя своё состояние в зависимости от поступающей к ним внешней информации. Одним из наиболее ярких представителей семейства алгоритмов машинного обучения являются нейронные сети – алгоритмы, хорошо предназначенные для адаптации к постоянно меняющимся внешним условиям [10].

Алгоритмы машинного обучения находят применение в АСОВ благодаря возможности обучаться на нормальном поведении участников рассматриваемой системы. Существует большое множество возможных подходов к внедрению машинного обучения в системы обнаружения вторжений [11], обусловленное отчасти

стремительным ростом интереса исследователей и разработчиков к применению машинного обучения в различных контекстах. Преимуществами использования алгоритмов машинного обучения являются их способность просто выражать нелинейные зависимости между переменными, а также возможность хранить своё состояние во времени. Тем не менее их реализации могут требовать значительных вычислительных мощностей, из-за чего полезность таких алгоритмов зависит от эффективности их программной реализации.

В рамках исследования разработана система обнаружения вторжений *NeuroTech* [12], в которой механизмом СОВ является обнаружение аномальных событий. Разработанная СОВ реализована на основе искусственной нейронной сети с глубинным обучением, для чего была использована выборка естественного сетевого трафика с ботнет-атаками, сгенерированная исследователями Чешского технического университета в Праге [13].

В дальнейшем СОВ испытывалась на реальном сетевом трафике открытого сервера (более двух миллионов записей о деятельности сети). Обучение СОВ проходило в гибридном режиме – наряду с обучением нормальному поведению сети, в нейронную сеть вводилась информациях о вредоносных действиях. В результате экспериментов точность нейронной сети варьировалась от 80% до 92%. Дальнейшая оптимизация нейронной сети возможна посредством обучения на значительных объёмах нормальной деятельности сети.

Существует множество различных подходов к реализации систем обнаружения вторжений, каждый из которых обладает собственным набором преимуществ и недостатков. СОВ, основанные на обнаружении злоупотреблений, хорошо подходят для использования в контекстах, где ожидается применение злоумышленниками хорошо известных атак. ЗСОВ также хорошо подходят для предприятий (банков), располагающих достаточным бюджетом для закупки или лицензирования продвинутых средств информационной безопасности. С другой стороны, СОВ, основанные на обнаружении аномалий, хорошо подходят для высоко динамичных или малоизвестных сред, для которых отсутствует объёмный корпус правил или сигнатур атак, а также для контекстов, в которых ожидаются атаки с использованием нетрадиционных векторов. Сегодня с развитием новых вычислительных методов, в том числе алгоритмов машинного обучения, растёт интерес к оптимизации алгоритмов обнаружения аномалий для реализации систем, отвечающим всем требованиям точности и полноты. В то же время, инновации в сфере практических реализаций СОВ зачастую связаны с применением машинного обучения и других развивающихся технологий во вспомогательной роли, а не в роли нового фундамента [14].

По этой причине применение машинного обучения в качестве основы новых СОВ остаётся приоритетным направлением исследования, заслуживающего внимания специалистов.

Литература

1. НАФИ. Российские компании потеряли не менее 116 млрд рублей от кибератак в 2017 году: Результаты опросов [Электронный ресурс]. – Режим доступа: https://nafi.ru/analytics/rossiyskie-kompanii-poteryali-ne-menee-116-mlrd-rubley-ot-kiberatak-v-2017-godu, свободный. – Загл. с экрана.

2. Lagarde, C. Estimating Cyber Risk for the Financial Sector [Электронный ресурс] / C Lagrade. – Режим доступа: https://blogs.imf.org/2018/06/22/estimating-cyber-risk-for-the-financial-sector, свободный. – Загл. с экрана.

3. Di Pietro, R. Intrusion Detection Systems. / R. Di Pietro, L. V. Mancini – New York City, NY, USA: Springer Science & Business Media, 2008. – 250 p.

4. Intrusion detection system: A comprehensive review / H.-J. Liao [et al.] // Journal of Network and Computer Applications. – 2013. – Vol. 36, Issue 1. – P. 16–24.

5. Anderson, D. Next-generation intrusion detection expert system (NIDES): A summary / D. Anderson, T. Frivold, A. Valdes. – Menlo Park, CA, USA: Computer Science Laboratory, SRI International, 1995. – 47 p.

6. Kumar, V. Signature Based Intrusion Detection System Using SNORT / V. Kumar, P. Om Sangwan. // International Journal of Computer Applications & Information Technology. – 2012. – Vol. I, Issue III. – P. 35–41.

7. Jensen, K. Coloured Petri Nets: Basic Concepts, Analysis Methods and Practical Use. Volume 1 / K. Jensen. – New York City, NY, USA: Springer Science & Business Media, 2013. – 236 p.

8. Anomaly-based network intrusion detection: Techniques, systems and challenges / P. García-Teodoro [et al.] // Computers & Security. – 2009. – Vol. 28. – P. 18–28.

9. Jyothsna, V. A Review of Anomaly based Intrusion Detection Systems / V. Jyothsna, V.V. Rama Prasad, K. Munivara Prasad. // International Journal of Computer Applications. – 2011. – Vol. 28, No. 7. – P. 26–35.

10. Гавриков, И. В. Обзор основных классов искусственных нейронных сетей и сфер их применений. / И. В. Гавриков, Д. В. Титаренко. // Актуальные исследования и инновации: материалы международной научно-практической конференции. – Самара, 2017. – С. 9–11.

11. Intrusion detection by machine learning: A review / C.-F. Tsai [et al.] // Expert Systems with Applications. – 2009. – Vol. 36, Issue 10. – P. 11994–12000.

12. Гавриков, И. В. Разработка системы обнаружения вторжений на основе искусственного интеллекта / И.В. Гавриков // Проблемы информационной безопасности: материалы IV Международной научно-практической конференции. – Симферополь–Гурзуф, 2018. – С. 141–142.

13. An empirical comparison of botnet detection methods / S. García [et al.] // Computers & Security. – 2014. – Vol. 45. – P. 100–123.

14. Sommer, R. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection / R. Sommer, V. Paxson. // 2010 IEEE Symposium on Security and Privacy. – Oakland, CA, USA: IEEE, 2010. – P. 305–316.