ОПРЕДЕЛЕНИЕ СТРАТЕГИИ АДМИНИСТРАТОРА ПО ПРОТИВОДЕЙСТВИЮ СЕТЕВЫМ АНОМАЛИЯМ НА ОСНОВЕ ТЕОРИИ ИГР

Русяев И.Л.

Русяев Иван Леонидович – магистрант,
кафедра вычислительной техники и защиты информации,
Оренбургский государственный университет, г. Оренбург

Аннотация: *организация безопасности компьютерной сети является неотъемлемой частью сетевого администрирования, при этом проблема выбора средств защиты информации полностью ложится на плечи администратора. Решение данной задачи возможно с помощью применения элементов теории игр, для этого разработана имитационная модель, сущность которой сводится к имитации взаимодействия субъектов в системе «нарушитель-защита» с целью автоматизации процедуры принятия решений при выборе оптимального комплекса средств защиты информации.*

Перед администраторами распределенных сетей, стоит задача обеспечить работоспособность этих сетей, их эффективное функционирование, а также целостность, доступность и конфиденциальность обрабатываемых данных, что можно рассматривать с точки зрения снижения риска аномальных режимов работы сети. Такие режимы называются сетевыми аномалиями и являются основными признаками сбоев в работе сети или действий злоумышленников. Анализируя причины возникновения, источники и степень опасности сетевой аномалии, можно своевременно выявить нарушение и снизить ущерб от ее возникновения [1].

На основе анализа научных публикаций [1-4] была построена классификация сетевых аномалий по причинам их возникновения, представленная на рисунке 1.

Рис. 1. Классификация сетевых аномалий по причинам возникновения

Согласно [5] все сетевые аномалии можно разбить на две большие категории: аппаратно-программные неисправности и нарушения безопасности. При администрировании распределенных сетей, несомненно, учитываются все возможные угрозы безопасности и функционирования сети, но при этом риск возникновения аномалии первой группы можно отнести к наименее вероятным, так как в основном они возникают из-за ошибок конфигурирования и нарушения производительности. Эти проблемы можно свести к минимуму путем соблюдения рекомендованного режима эксплуатации оборудования, правильного его конфигурирования и периодичных проверок каналов связи на отсутствие физических дефектов и сохранение пропускной способности.

Ко второй же группе относятся случайные или намеренные действия лиц, повлекшие за собой возникновение аномального режима работы сети, который, в свою очередь, может привести как к нарушению производительности распределенной сети, так и к полной потере доступа к сетевым ресурсам.

Если аномальный режим работы возник не из-за случайной ошибки пользователя или администратора, а из-за целенаправленных действий злоумышленника то эти действия с уверенностью

можно назвать сетевой атакой. Целью любой сетевой атаки является получение злоумышленником доступа к конфиденциальной информации, либо создание условий, при которых легитимные пользователи не могут получить доступ к данной информации или системным ресурсам, что вызывает простой службы и приносит экономические потери владельцу распределенной сети.

По данным аналитического центра компании InfoWatch [6], проводившего глобальное исследование утечек конфиденциальной информации в 2016 году, показатель утечек информации относительно показателей на 2015 год возросло на 3,6% - рисунок 2. При этом доля утечек через «сетевой» канал возросла на 11,6% и составила 69,5% от общего числа утечек конфиденциальной информации.

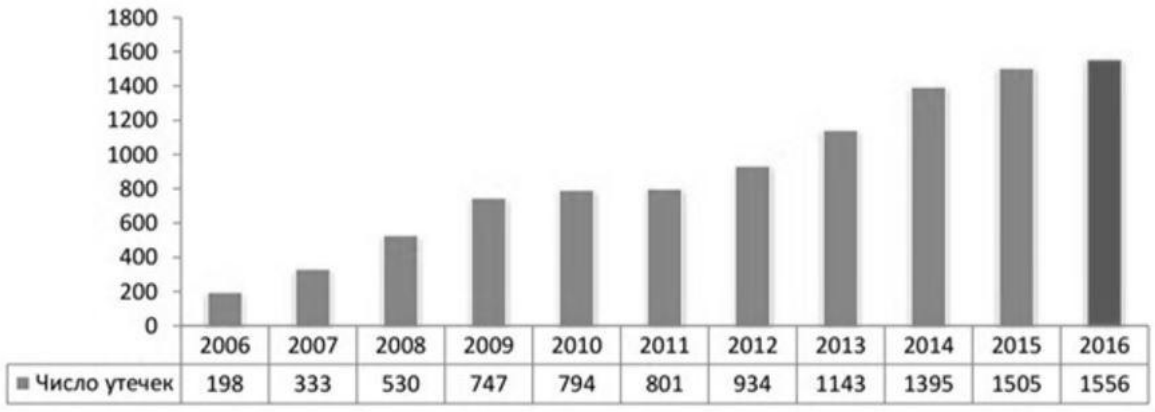

Рис. 2. Число зарегистрированных утечек информации, 2006 - 2016 г.

Опираясь на представленные данные, можно с уверенностью сказать, что наиболее опасными являются аномалии, возникшие в результате проведения сетевой атаки. Поэтому задача определения стратегии администратора по противодействию сетевым аномалиям имеет необходимый и своевременный характер.

Существуют различные подходы к определению стратегии администратора, одним из них является применение теории игр. Данная математическая теория появилась в середине XX века и зарекомендовала себя в экономике, её применение актуально и в наши дни.

В представленной работе рассматривается теоретико-игровой подход, который позволяет исследовать взаимоотношения злоумышленника и администратора – как субъектов конфликта (некоторого игрового процесса).

Матричная игра – это одношаговая математическая игра двух сторон, для ее реализации необходимо однозначно определить стратегии субъектов взаимодействия, в частности стратегии злоумышленника и администратора. Первым этапом определения стратегии противодействия является построение модели вероятных сетевых атак. Тогда можно считать, что реализация данных сетевых атак и будет являться множеством стратегий злоумышленника, а сопровождающий их ущерб будет являться целью исследования, независимо от начальных целей нарушителя. На втором этапе определяются методы борьбы с сетевыми аномалиями, и строится функциональная «матрица игры», которая позволит определить оптимальную стратегию администратора, при которой ущерб от реализованных сетевых атак будет сведен к минимуму. Исходя из этого, игровой процесс также разбивается на две части, сначала определяется базовый набор мер противодействия необходимых для достижения минимально допустимого уровня риска безопасности сети, а затем определяется оптимальный комплекс средств защиты распределенной сети.

На основе анализа публикации [7] была построена функциональная матрица $N\{S_t,Q_k\}$ в системе «нарушитель-защита», которая позволяет определить базовый набор средств защиты распределенной сети, с помощью оценки «опасности атаки» и имеет следующий вид:

$$N\{\ S_t, Q_k\ \} = c_{tk} = \begin{pmatrix} c_{11} & \cdots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{m1} & \dots & c_{mn} \end{pmatrix},\ c_{tk} = [0;1]; \qquad (1.1)$$

где S_t – множество сетевых аномалий;

Q_k – множество мер противодействия сетевым аномалиям;

c_{tk} – функциональный показатель мер противодействия.

Параметр «опасность атаки» (ОА) может принимать значения от «-10» до «10». Если опасность атаки (ОА) будет принимать положительные значения (от 0 до 10), то риск безопасности компьютерной системы велик, и необходимо принять меры по противодействию данной сетевой атаке. Если же

параметр принимает отрицательные значения, то атака незначительна или перекрывается существующей системой защиты и не требует дополнительных мер противодействия:

$$OA \in [-10;10], \quad OA_t \geq 0 \Rightarrow \begin{cases} c_{tk} = 1, \ Q_k \in \text{B} \\ c_{tk} = 0, \ Q_k \notin \text{B} \end{cases}; \tag{1.2}$$

где В – базовый набор мер противодействия.

Данная методика оценки риска безопасности компьютерной системы подробно представлена в научной публикации [8]. Функциональная матрица мер противодействия сетевым аномалиям представлена на рисунке 1.

Таблица 1. Функциональная матрица мер противодействия

Сетевая Атака / Мера противодействия	Снифинг трафика	IP-Спуфинг	Dos/DDos	Атака уровня приложений	Сетевая разведка	Вредоносное ПО
IDS/IPS	0	1	1	1	1	1
Межсетевой экран	0	1	1	1	1	0
Антивирус	0	0	0	1	0	1
VPN	1	1	0	0	0	0
Опасность атаки	OA_1	OA_2	OA_3	OA_4	OA_5	OA_6

Представленная матрица отражает функциональные особенности средств защиты сетей и позволяет оценить необходимость их использования на существующей системе. Например, если значения опасности атаки OA_1, OA_2 и OA_4 будут отрицательными, значит, использование дополнительных средств VPN будет неоправданным, объяснить это можно тем, что конфиденциальная информация не выходит за физические границы сети, либо наличием действующей системы шифрования данных в сети.

В случае если все значения ОА будут положительными, тогда базовый набор средств будет включать все представленные методы противодействия и их применение позволит построить многоуровневую систему защиты, которая является наиболее эффективной в настоящее время.

Второй этап матричной игры заключается в определении оптимального комплекса средств защиты распределенной сети, исходя из базового набора средств *B*. Для выполнения этой задачи необходимо построение расширенной таблицы взаимодействия стратегий злоумышленника и администратора. В данном случае реализация сетевых атак приводит к возникновению угроз безопасности компьютерной сети, которые будут являться множеством стратегий нарушителя $X = \{X_1, X_2, \ldots X_m\}$, а сопровождающий их ущерб – целью атаки, независимо от начальных целей нарушителя. Средства защиты информации будут являться стратегиями администратора $Y = \{Y_1, Y_2, \ldots Y_n\}$, а M_j – стоимость j-й стратегии.

Для формализации задачи использованы условные обозначения, приведенные в таблице 2.

Таблица 2. Условные обозначения математической модели

Символ	Обозначение
X_i	i-я стратегия нарушителя, i=1, ... n;
Y_j	j-я стратегия администратора , j=1, ... m;
a_{ij}	результат взаимодействия i-й стратегии нарушителя и j-ой стратегии администратора;
$K_{НУj}$	коэффициент нейтрализации угроз для j-й стратегии администратора;
$P_{испj}$	экономическая целесообразность использования j-й стратегии администратора;
$F\{x\}$	процедура принятия решения об оптимальности j-й стратегии администратора;
M_j	Стоимость j-ой стратегии администратора;

SZI{Z}	множество оптимальных стратегий Z_j, образующих оптимальный комплекс.

Математическое описание процедуры определения оптимального комплекса S*ZI* имеет следующий вид:

$$A\{ X_i, Y_j \} = a_{ij} = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}; \quad (1.3)$$

$$F\{K_{HYj},P_{ucnj}\}=M_j/\{\sum_{i=0}^{m} a_{ij}\}, j = 1,n; \quad (1.4)$$

$$Z_j \in SZI: F\{K_{HY},P_{ucn}\}=min\ F\{K_{HYj},P_{ucnj}\}, \quad (1.5)$$
$$при\ max(K_{HYj}),\ P_{ucnj}<1,\ \ j=1,n.$$

Данная модель применяется для нахождения оптимального комплекса средств защиты информации, позволяющего максимально эффективно противодействовать сетевым аномалиям. Этот комплекс СЗИ и будет в свою очередь являться стратегией администратора.

Для построения матрицы игры необходимо на основе множества сетевых аномалий выделить угрозы безопасности компьютерной системы, которые будут являться стратегиями нарушителя. Перечень вероятных угроз: 1) несанкционированный доступ в сеть; 2) кража конфиденциальной информации (перехват); 3) отказ в обслуживании (Dos/DDos); 4) заражение вредоносным ПО через сеть; 5) заражение вредоносным ПО через съемные носители; 6) кража банковских реквизитов через анализ трафика; 7) перехват паролей; 8) выведение системы из строя; 9) сетевая разведка; 10) эксплуатация уязвимостей; 11) фишинг; 12) кража производительности; 13) модификация трафика; 14) ip-спуфинг; 15) искажение данных; 16) атака «человек посередине»; 17) атака на средства защиты.

Для составления множества стратегий администратора безопасности необходимо проанализировать современный рынок средств защиты. Для этого проведен анализ данных первого в России независимого информационно-аналитического центра «Anti-Malware.ru» [9]. Множество средств защиты информации, выбранных для разработки имитационной модели, имеют высокий рейтинг по итогам тестирования аналитическим центром. Перечень исследуемых средств защиты: 1) McAfee Network Security Platform; 2) Cispo IPS-4240-K9; 3) HP Tipping Point IPS; 4) Киберсейф межсетевой экран; 5) VipNet Office Firewall; 6) Check Point 4800; 7) Kaspersky Endpoint Security для бизнеса Расширенный; 8) Symantec Endpoint Protection Small Business Edition; 9) Dr.Web «Стандарт» для бизнеса; 10) ИКС Стандарт VPN; 11) АПКШ «Континент»; 12) Cisco 1720.

С учетом перечня вероятных угроз была построена таблица соответствия функциональных качеств СЗИ и вероятных угроз объекта защиты, таблица 3.

Таблица 3. Соответствие функциональных качеств СЗИ и вероятных угроз объекта защиты

Угроза / СЗИ										10	11	12	13	14	15	16	17
1										+		+	+	+	+		+
2										+		+	+	+	+		+
3										+	+	+	+	+	+		+
4												+		+			
5												+		+			+
6												+		+		+	+
7										+	+						+
8										+			+				+
9										+	+						+
10													+	+		+	
11													+	+		+	+
12													+	+		+	

Представленная таблица однозначно описывает взаимодействие противоборствующих сторон и позволяет формализовать процесс выбора оптимальной стратегии администратора на основе теории игр.

В рамках поставленной задачи производится имитация взаимодействия в системе «нарушитель-защита», целью которой является определение стратегии администратора по противодействию сетевым аномалиям для снижения риска аномальных режимов работы распределенной сети, а, следовательно, и снижение ущерба от их воздействия на работоспособность системы.

Вектор входных данных имитационной модели V состоит из следующих параметров: множество сетевых атак S, множество мер противодействия Q, множество стратегий администратора (средств защиты информации) Y, множество стратегий нарушителя (угрозы от реализации атак) X, множество значений ущерба от реализации стратегий нарушителя L и множество значений опасности атак распределенной сети ОА.

Вектор выходных данных W состоит из: оптимального комплекса средств защиты SZI', стоимости оптимального комплекса M и значения остаточного ущерба $U_{ост.}$

Схема имитационной модели определения оптимального комплекса средств защиты информации на основе элементов теории игр представлена на рисунке 3.

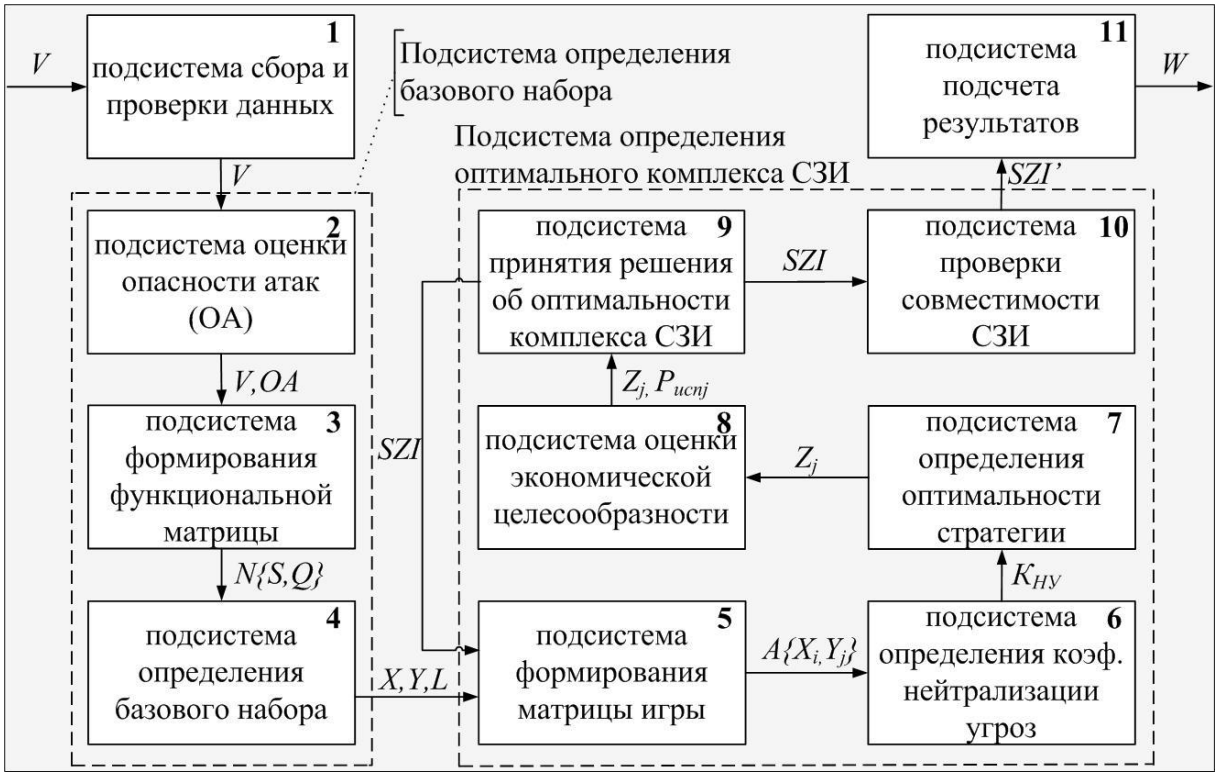

Рис. 3. Структурная схема имитационной модели определения оптимального комплекса СЗИ

Разработанная имитационная модель позволяет имитировать взаимодействие субъектов в системе «нарушитель-защита» и на основе этого определять стратегию администратора, в частности при выборе средств защиты информации для снижения риска возникновения аномальных режимов работы распределенной сети. Данная модель универсальна и может применяться для исследований аналогичных игровых ситуаций в задачах защиты информации.

Список литературы

1. *Оладько В.С., Микова С.Ю., Нестеренко М.А., Садовник Е.А.* Причины и источники сетевых аномалий // Молодой ученый, 2015. № 22. С. 158-161.
2. *Шелухин О.И., Сакалема Д.Ж., Филинова А.С.* Обнаружение вторжений и компьютерные сети. / О.И. Шелухин. М.: Горячая линия-Телеком, 2013. 220 с.
3. *Кучер В.А., Магомадов А.С., Чигликова Н.Д., Дьяченко Р.А.* Системы устранения сетевых аномалий и методики построения их архитектуры // Научный журнал КубГАУ, 2015. № 110 (06)
4. *Микова С.Ю., Оладько В.С., Нестеренко М.А.* Подход к классификации аномалий сетевого трафика // Инновационная наука, 2015. № 11. С. 78-80.
5. *Левонский Д.К., Фаткиева Р.Р.* Разработка системы обнаружений аномалий сетевого трафика // Научный вестник НГТУ, 2014. № 3. С. 108–114.
6. Глобальное исследование утечек конфиденциальной информации в 2016 году // Аналитический центр InfoWatch. [Электронный ресурс]. Режим доступа: https://www.infowatch.ru/report2016 / (дата обращения: 03.05.2017).
7. Типы сетевых атак, их описание и средства борьбы // [Электронный ресурс]. Режим доступа: http://lagman-join.narod.ru/spy/CNEWS/ cisco_attacks.html/ (дата обращения: 21.06.2017).

8. *Гуц А.К.* Теория игр и защита компьютерных систем: учебное пособие / А.К. Гуц, Т.В. Вахний. Омск: Издательство ОмГУ, 2013. 160 с.
9. Anti-Malware – независимый информационно-аналитический центр. [Электронный ресурс]. Режим доступа: http://www.anti-malware.ru/about/ (дата обращения: 21.06.2017).