**Инженерный вестник Дона**, №1 (2019)
ivdon.ru/ru/magazine/archive/n1y2019/5755

# Обеспечение компьютерной безопасности с использованием метода «безопасность через неясность»

*М.А Ганжур, А.П. Ганжур, И.М. Борисенко*
*Донской государственный технический университет, Ростов-на-Дону*

**Аннотация:** Обеспечение компьютерной безопасности в наше время является одной из ключевых задач. Атаки на оборудования в сети происходят постоянно и наносят большой ущерб целостности данных. Существует множество методов обеспечения компьютерной безопасности, одним из которых является метод «безопасности через неясность», дающий положительные результаты в работе веб-серверов.
**Ключевые слова:** компьютерная безопасность, безопасность через неясность, криптография, расшифровка, настройка веб-серверов.

## Введение

Существует множество методов обеспечения компьютерной безопасности, одним из которых является «безопасность через неясность». Данный метод основывается на описании состояния, в котором системный администратор предполагает, что злоумышленник ничего не знает о настройке сети, компьютера или программы.

## Цель исследования

Процесс вывода знаний в машинах нечеткого вывода дуальной сетью Петри, позволяющей получать нормализованные данные в результате работы системы при борьбе со злоумышленниками [1].

## Основная часть исследования

Один простой пример: мы помещаем важные документы своей компании на внутренний веб-сервер без защиты паролем на страницах. Вместо того, чтобы полагаться на классические методы аутентификации, администратор сети полагается на волю случая, считая, что никто не узнает об этом веб-сервере, кроме внутренних сотрудников компании, которым известно о наличии сервера. Существуют следующие инструменты сетевого обнаружения: cheops, firewalk, snmpwalk и nmap, которые могут найти практически любой веб-сервер в сети. Ошибка системных администраторов в

том, что они полагаются на неизвестность, как единственный метод контроля доступа. Хотя некоторые злоумышленники никогда не будут тратить силы на поиск данного веб-сервера, другие могут использовать его для баловства и могут получить доступ к информации, которую мы хотели спрятать.

Еще одним из примеров метода «безопасность через неясность», является установка нестандартного порта при обращении к веб-серверу. Вместо обычного порта 80, например, используют 8000. Злоумышленник может решить проверить все порты, включая и 8000. Используя данный метод, системный администратор беспечно полагается на метод «безопасность через неясность», так взломщик, использующий Nessus (Nessus — программа для автоматического поиска известных изъянов в защите информационных систем), обнаружит и данное изменение. В примере Nessus сканер смотрит на первую часть сообщения, и идентифицирует сервер, независимо от местоположения порта. Таким образом, многие злоумышленники смогут найти доступ и на этот веб-сервер.

Неизвестность в качестве единственного метода защиты не работает как метод контроля доступа. Злоумышленник может за счет опросов найти почти всё, опросив машины, находящиеся по соседству в сети, маршрутизаторы и саму машину-цель несанкционированного доступа. Это возможно за счет запуска активных сканеров или пассивного анализатора трафика - так называемого сниффера. Также возможны атаки с помощью «социальной инженерии». Злоумышленник может получить или угадать информацию, которую мы скрываем, особенно если это так же просто, как прослушивать порт нашего веб-сервера, т.е. мы не реализуем достаточный уровень безопасности. Метод обеспечения безопасности, осуществляемый исключительно через неясность, является недостаточным.

Обычно мы просто говорим о том, насколько сильна неясность и насколько легко ее можно изменить. Исходная идея - безопасность,

реализованная исключительно через неясность, недостаточна. Такое суждение исходило от критики некоторых криптосистем. Криптографы обнаружили, что некоторые слабые криптосистемы скрывали криптоалгоритм как свою единственную защиту. Когда атакующий криптограф смог разгадать алгоритм с помощью обратной инженерии, то он смог дешифровать все сообщения, зашифрованные им. В шифре Цезаря каждое сообщение кодируется просто путем изменения каждой буквы исходного текста в третью букву после нее в заранее выбранном алфавите. Таким образом, A становится D (в случае с английским алфавитом), B становится E и т. д. Слово «security» становится «vhfxulwb». Как только мы знаем алгоритм шифрования, мы можем разгадать шифр, просто заменив каждую букву буквой алфавита, которая предшествует ей на 3. Система становится слабой, как только мы узнаем алгоритм шифрования. Безопасность системы заключалась только в секретности или неясности алгоритма. Использование модификации данного алгоритма с помощью варьирования ключа от 1 до 255, принимая 8-битную систему, позволит быстро скомпрометировать данные с использованием метода «грубой силы». С другой стороны, использование 40-битного шифрование (более 1 триллиона возможных ключей), не позволяет так легко перехватить и дешифровать сообщения. Хорошие криптосистемы дают возможность своим пользователям не бояться, что их сообщения прочитает злоумышленник. Рассмотрим другую ситуацию, входя в операционную систему, электронную почту или личные страницы сайта/приложения, необходимо ввести пароль. Если пароль не раскрыт, то все данные защищены. Таким образом, если вернуться к криптографии главным вопросом является маскировка ключей, а не алгоритма.

Теперь предположим, что на веб-сервер компании установили хороший пароль или использовали какой-либо другой, более совершенный метод

аутентификации. Далее размещаем сайт на сервере SSL, идентифицируя пользователей сертификатами на стороне клиента. Теперь мы достигли достойного контроля доступа. Местоположение сервера и номер порта не могут служить в качестве метода аутентификации, а знание данной информации злоумышленником не повредит безопасности сервера.

Рассмотрим атаки веб-серверов. Одним из атакующих элементов являются так называемые детские скрипты (от англ. script-kiddie). Скрипты-это программы, разработанные пользователями слишком неопытными, не понимающими механизма их действия, для атаки компьютерных систем и сетей. Целью является лишь попытка произвести впечатление на друзей или получить похвалу от сообществ компьютерных энтузиастов. Например, если детский скрипт имеет эксплойт против IIS версии 4.1, сканирующий Интернет в поисках IIS. У данного сканера часто такой алгоритм:

— Проверка, открыт ли порт 80 на каждом целевом компьютере.

— Если необходимо, подключиться к порту 80 и проверить строку версии.

— Записать IP-адрес этого уязвимого веб-сервера

— Если мы используем веб-сервер на порту, отличном от 80, он избегает этого сканирования.

Злоумышленники не все используют низкоуровневые инструменты. Если злоумышленник получил сканер, который проверяет несколько портов или даже проверяет каждый порт, он также может попытаться использовать тривиальный подход «пулемет», стреляя своим эксплойтом в каждый открытый порт, не проверяя, уязвим ли веб-сервер или нет.

Неясность может помочь блокировать некоторое количество атак, например, от «детей» с обычными низкоуровневыми инструментами или злоумышленников, которые слишком ленивы, чтобы проверить все порты на машине. Мы не используем неизвестность для аутентификации - мы просто

используем ее, чтобы помочь существующей хорошей системе аутентификации.

Давайте подумаем о том, что мы увидим, если мы следили за сетевым подключением веб-сервера. В случае, когда мы помещаем наш веб-сервер на общий порт, порт 80, информационный зонд нашего злоумышленника, например, IIS, анализирует брандмауэр/ журналы маршрутизаторов, как и любой другой веб-запрос, поступающий в машину. Наш нападающий это знает и вполне доволен, потому что у него мало шансов быть замеченным при его информационном зонде. Когда мы помещаем наш веб-сервер в порт 253, злоумышленнику, как правило, придется сканировать множество портов на целевом веб-сервере, чтобы найти его. Вместо того, чтобы сделать тихий запрос к порту 80 как цели, ему придется отправить по крайней мере один пакет на многие целевые порты, чтобы найти открытые, а затем установить соединения с каждым из открытых, пока не найдет тот, который запускает веб-сервер. Его атака только стала еще «громче». Многие детекторы сканирования портов, в том числе Port Scan Attack Detector Mike Rash, отслеживают, как одинаковые пакеты отправляются на несколько разных портов машины, и предупреждают об этом.

Итак, есть еще одно преимущество использования неясности. Неизвестность потенциально замедляет атакующего. Утаивая информацию о нашей среде, мы вынуждаем атакующего, возможно, прилагать больше усилий, чтобы узнать эту информацию, прежде чем он сможет выполнить свою атаку. Это дает нам больше шансов наблюдать за атакой.

Запуск сканера портов значительно замедляет работу. Это особенно выгодно, когда злоумышленник сканирует каждую машину в домене, так как он должен генерировать намного больше запросов и ждать еще больше ответов, просто чтобы найти сервер. Чтобы получить представление об этом, рассмотрим домен из 200 машин. Обычно он просто делает около 50-200

запросов, чтобы найти веб-сервер, в худшем случае из 200 запросов. Предположим, что он сканирует 1000 портов, ища открытые порты на каждой машине, то есть 50 000 - 200 000 запросов. Так он может быть очень тщательным и проверить все 65535 возможных портов, в худшем случае около 13 миллионов запросов. Это довольно сильно замедлит его и сделает его целевое сканирование довольно «громким».

Используя композиционные правила вывода для машины нечеткого вывода, представляемые в виде [2]:

$$\frac{F \rightarrow G}{F'}$$
$$G'$$

Вывод $G'$определяется из свертки $max - min$ нечеткого множества $F'$ и отношения $R$, где:

$R = F \times G$ [2];

$U = \{u1, u2, \ldots, um\}; V = \{ v1, v2, \ldots, vm \};$

$F, F' \subset U; G, G' \subset V.$

Таким образом:

$Gi' = max\{min(\mu(fi), min((ui),(vi))), min(\mu(fi+1), min((ui+1), (vi+1)))\};$

$Gi' = min\{ max\ \mu(fi), max((ui),(vi))), max(\mu(fi+1), max((ui+1), (vi+1)))\}.$

Из полученного выражения представим ветвь вывода, соответствующую одной из функций принадлежности выводимого знания, в виде нечеткого вывода дуальной сети Петри. Нечеткие иерархические сети Петри - это двудольный ориентированный граф. Это сочетание двух типов объектов, а именно позиции и перехода, представленных в виде кругов и прямоугольников соответственно. Позиции могут содержать маркеры, связанные со степенью доверия, выглядящие как точка значения в диапазоне [0,1]. Направленные дуги соединяют входные позиции с переходами и переходы к выходным. Каждый переход содержит значение фактора

определенности (μ), которое находится в промежутке [0,1] и пороговое значение (τ). Переход срабатывает, если μ > τ. После срабатывания перехода маркер передается от входного перехода к выходному, предварительно рассчитывая переход на выходную позицию. Структура FPN определена 9 параметрами.

*FPN = ( P, T, I, O, D, W, U, Th, M)* где:

$P = (p_1, p_2, \ldots p_m)$ конечное множество позиций. Каждый элемент $p_i=(p_i^1;p_i^0)$состоит из $p_i^1$- прямой позиции, и $p_i^0$- инверсной позиции; с выполнением условия $p_i=p_i^1 \cup p_i^0$;

$T = (t_1, t_2, \ldots t_n)$ - конечное множество переходов;

$I$: $P \times T \rightarrow [0,1]$ - входная матрица с порядком $m \times n$. Если позиция *pi* соединена дугой с переходом *tj*, тогда элемент матрицы $I$, $I_{ij} = 1$, в противном случае $I_{ij} = 0$;

$O$: $T \times P \rightarrow [0,1]$ - выходная функция переходов с порядком $m \times n$. Если переход *tj* соединен дугой с позицией *pi*, тогда элемент матрицы $O$, $O_{ij} = 1$, в противном случае $O_{ij} = 0$;

$D = \{d1, d2, \ldots dm\}$ представляет набор утверждений $\infty: P \rightarrow [0,1]$ - функция, отображающая места вещественных значений в пределах [0 1].

$\beta: P \rightarrow D$-функция, которая отображает места утверждения.

$W: P \times T \rightarrow [0,1]$ является входной функцией и представлен в виде матрицы размером $m \times n$. В матрице входным значением $W_{ij} \in [0,1]$ является вес, связанный с местом ввода. Для одного перехода сумма весов для всех входных мест =1.

$U: T \times P \rightarrow [0,1]$ - функция вывода и представлен в виде матрицы размером $m \times n$. Входное значение в матрице $U$, $\mu ij \in [0,1]$ равно значению фактора определенности $(\mu)$, определяющего переход *tj, что* может влиять на его выходные места *pi;*

*Th: O → [0,1]* - функция вывода и представлен в виде матрицы $m \times n$, запись в матрице $\tau_{ij} \in [0,1]$ показывает порог выхода в позиции $p_i$ от перехода $t_j$ *сайт* $\tau_{ij} = \infty$ , если это не выходная позиция.

*M* динамический входной сигнал и сразу влияние динамического поведения*DFPN.M = (∞(p1), ∞ (p2) ,..., ∞ (pm))*$^T$ начальная маркировка обозначается $M_0$.

Структура сети Петри содержит только фрагменты, соответствующие продукционным правилам П1, П2, П3, П4, П5:

П1: «ЕСЛИ А, ТО В» ( $A \to B$ );

П2: «ЕСЛИ А и В и … и С, ТО D» ($A\&B\&...\&C \to D$);

П3: «ЕСЛИ А или В или … или С, ТО D» $(A \vee B \vee ... \vee C \to D)$;

П4: «ЕСЛИ А, ТО В и С и … и D» ($A \to B\&C\&...\&D$);

П5: «ЕСЛИ А, ТО или В или С или…или D» $(A \to B \vee C \vee ... \vee D)$

Задавая значения дерева событий, можно рассчитать возможность атаки на сетевое оборудование злоумышленником (Рис.1).

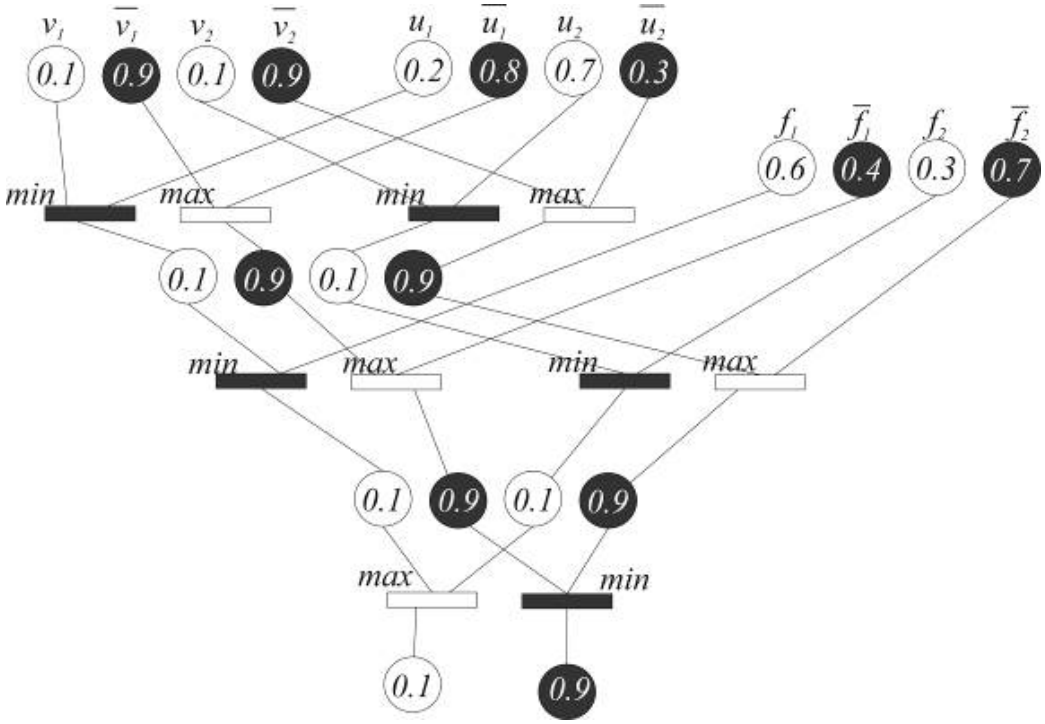


Рисунок 1 – Дуальная сеть Петри нечеткого вывода знаний атаки оборудования

Здесь $\mu\ (g1)$ является элементом матрицы $|\mu\ (g1),\ \mu(g2),\ldots,)\ \mu\ (gm)|$ функций принадлежности выводимого знания $G'$.

Для разметки сети Петри нечеткого вывода знаний необходимо изменить разметку входных позиций, помеченных функциями принадлежности лингвистических переменных из отрезка [0,1] за счет нормализации в целочисленный отрезок [0, 10], или [0, 100], в зависимости от используемой разрядности. Полученные в результате вывода целочисленные разметки выходных позиций, используя обратную операцию, переводятся в дробные значения, соответствующие функциям принадлежности выведенных знаний.

## Заключение

Метод «безопасность через неясность» замедляет атакующего, также дополнительная неясность ограничивает возможность взлома защищаемого объекта со стороны неопытных взломщиков, использующих низкоуровневые инструменты. Кроме того, метод «безопасность через неясность» может действительно заставить злоумышленника отказаться от атаки или демаскировать себя в ходе атаки. В соответствии с композитным правилом, в работе показана конструкция дуальной нечеткой сети Петри, которая предполагает использование переходов max и min. Переход от классических сетей Петри к дуальным нечетким сетям реализует нечеткие знания логического вывода, что позволяет решить вопросы, связанные с анализом угроз, исходящих от злоумышленников, а также обеспечивает эффективность избранных методов защиты от них.

## Литература

1. Змитрович А.И. Интеллектуальные информационные системы. Мн.: НТООО «ТетраСистемс», 1997. С. 368.

2. Фатхи Д.В., Фатхи Дм.В., Фатхи Д.В. Функция достижимости и сетевая производная нечеткой сети Петри на основе μ-значной логики //

Математические методы в технике и технологиях – ММТТ-19: сб.трудов XIX Междунар. науч. конф.: в 10-и т. Т.6/ под общ. ред. В.С.Балакирева. – Воронеж, Воронеж. гос. технол. акад., 2006. С. 244.

3. Евсин В.А., Тихонов Н.А., Воробьев С.П. Разработка модуля оптимального размещения информационных ресурсов на узлах вычислительной сети: описание реализуемых методов и структур данных // Инженерный вестник Дона, 2019, №1. URL:ivdon.ru/ru/magazine/archive/n1y2019/5493

4. Н. В. Берёза Современные тенденции развития мирового и российского рынка информационных услуг // Инженерный вестник Дона, 2012, №2. URL: ivdon.ru/magazine/archive/n2y2012/758

5. M.A. Ganzhur, A.P. Ganzhur, O.V. Smirnova. Modeling of critical systems implementing negative events using dual Petri nets. MATEC Web of Conferences Volume 226 (2018), XIV International Scientific-Technical Conference “Dynamic of Technical Systems” (DTS-2018). URL:doi.org/10.1051/matecconf/201822604001

6. N. Marković, J. Živanić, Z. Lazarević, B. Iričanin. The Mathematical Model for Analysis and Evaluation of the Transient Process of the three–phase Asynchronous Machine Performance. Serbian journal of electrical engineering (DTS-2018) URL:journal.ftn.kg.ac.rs/Vol_15-3/05-Markovic-Zivanic-Lazarevic-Iricanin.pdf

7. Зотов А.И., Ганжур М.А., Авакьянц А.В. Характеристика управленческой структуры и системы прохождения команд // Проблемы современного педагогического образования. Сер. Педагогика и психология. - 2018. - Вып. 58, ч. 3. - С. 111-116.

8. Ганжур М. А, Ганжур А. П. Моделирование экспертных систем на основе дуальных сетей Петри / // Системный анализ, управление и обработка информации: тр. VIII

Междунар. науч. конф., с. Дивноморское, 8-13 окт. 2017 г. В 2-х т. / Дон. гос. техн. ун-т. - Ростов н/Д.: ДГТУ, 2017. - Т. 1. - С. 211-213

9. Зотов А. И., Ганжур М. А. Моделирование безопасности управленческих структур // Системный анализ, управление и обработка информации: тр. VIII Междунар. науч. конф., с. Дивноморское, 8-13 окт. 2017 г. В 2-х т. / Дон. гос. техн. ун-т. - Ростов н/Д.: ДГТУ, 2017. - Т. 1. - С. 163-167.

10. Урубкин М. Ю., Ганжур М. А., Ковальский Б. А. Применение сетей Петри при моделировании процесса функционирования сетей // Актуальные вопросы и основы международного сотрудничества в сфере высоких технологий: сб. ст. по итогам Междунар. науч.-практ. конф., 19 дек. 2017 г. / Агентство междунар. исследований. - Стерлитамак: АМИ, 2017. - С. 173-176.

## References

1. Zmitrovich A.I. Intellektual'nye informacionnye sistemy [Intelligent Information Systems]. Mn.: NTOOO «TetraSistems», 1997. P. 368.

2. Fathi D.V., Fathi Dm.V., Fathi D.V. Matematicheskie metody v tehnike i tehnologijah – MMTT-19: sb.trudov XIX Mezhdunar. nauch. konf.: v 10-i t. T.6. Pod obshh. red. V.S.Balakireva. Voronezh, Voronezh. gos. tehnol. akad., 2006. P. 244

3. Evsin V.A., Tikhonov N.A., Vorobyev S.P. Inženernyj vestnik Dona (Rus), 2019, №1. URL: ivdon.ru/ru/magazine/archive/n1y2019/5493

4. Bereza N.V. Inženernyj vestnik Dona (Rus), 2012, №2. URL: ivdon.ru/magazine/archive/n2y2012/758

5. M.A. Ganzhur, A.P. Ganzhur, O.V. Smirnova. MATEC Web of Conferences Volume 226 (2018), XIV International Scientific Technical Conference “Dynamic of Technical Systems” (DTS-2018). URL:doi.org/10.1051/matecconf/201822604001

6. N. Marković, J. Živanić, Z. Lazarević, B. Iričanin. Serbian journal of electrical engineering (DTS-2018) URL:journal.ftn.kg.ac.rs/Vol_15-3/05-Markovic-Zivanic-Lazarevic-Iricanin.pdf

7. Zotov A.I., Ganzhur M.A., Avakyants A.V. Problemy sovremennogo pedagogicheskogo obrazovanija. Ser. Pedagogika i psihologija. 2018. Vyp. 58, ch. 3. pp. 111-116.

8. Ganzhur M. A., Ganzhur A. P. Sistemnyj analiz, upravlenie i obrabotka informacii: tr. VIII Mezhdunar. nauch. konf., s. Divnomorskoe, 8-13 okt. 2017 g. V 2-h t. Don. gos. tehn. un-t. Rostov n/D.: DGTU, 2017. T. 1. pp. 211-213.

9. Zotov A. I., Ganzhur M. A. Sistemnyj analiz, upravlenie i obrabotka informacii: tr. VIII Mezhdunar. nauch. konf, s. Divnomorskoe, 8-13 okt. 2017 g. V 2-h t. Don. gos. tehn. un-t. Rostov n/D.: DGTU, 2017. T. 1. pp. 163-167.

10. Urubkin M.Yu., Ganzhur M.A., Kovalsky B.A. Aktual'nye voprosy i osnovy mezhdunarodnogo sotrudnichestva v sfere vysokih tehnologij: sb. st. po itogam Mezhdunar. nauch.-prakt. konf., 19 dek. 2017 g. Agentstvo mezhdunar. issledovanij. Sterlitamak: AMI, 2017. pp. 173-176.