УДК 519.85
DOI: 10.26102/2310-6018/2023.43.4.031

Разработка концепции и инструментария моделирования процессов тестирования веб-приложений методом фаззинга с помощью динамических байесовских сетей

Т.В. Азарнова, П.В. Полухин✉

Воронежский государственный университет, Воронеж, Российская Федерация

Резюме. Обеспечение устойчивости функционирования веб-приложений относительно различных угроз безопасности играет важнейшую роль в развитии современных технологий информационного обеспечения промышленных предприятий, финансовых структур и организаций сферы услуг. Это объясняет высокую актуальность разработки новых научно обоснованных эффективных вычислительных методов, алгоритмов и проблемно-ориентированных программ для тестирования веб-приложений со сложной функциональной структурой внутреннего и внешнего взаимодействия, реализующих возможности потоковой обработки данных, формируемых по результатам каждого из шагов тестирования, и применение полученных результатов в процессе управления тестированием веб-приложений. В статье описана концепция моделирования процессов тестирования, исследования полученных моделей и разработки алгоритмов анализа и прогнозирования, базирующаяся на формализованном аппарате динамических байесовских сетей. Предложенные в работе байесовские модели, построенные на основе статистического обучения, позволяют определить временные связи для каждого из параметров, определяемых в процессе выполнения процедуры тестирования, и предоставляют возможность прогнозировать результаты тестирования путем выполнения процедуры имитационного моделирования методами вероятностного вывода.

***Ключевые слова*:** уязвимости веб-приложений, байесовская сеть, задачи вероятностного вывода, процесс тестирования, метод Монте Карло с применение цепей Маркова, алгоритм многочастичного фильтра.

Для цитирования: Азарнова Т.В., Полухин П.В. Разработка концепции и инструментария моделирования процессов тестирования веб-приложений методом фаззинга с помощью динамических байесовских сетей. *Моделирование, оптимизация и информационные технологии.* 2023;11(4). URL: https://moitvivt.ru/ru/journal/pdf?id=1479 DOI: 10.26102/2310-6018/2023.43.4.031

Development of a concept and tools for modeling web application testing processes using fuzzing using dynamic Bayesian networks

T.V. Azarnova, P.V. Polukhin✉

Voronezh State University, Voronezh, the Russian Federation

Abstract. Ensuring the sustainability of web applications with respect to various security threats plays a crucial role in the development of modern information support technologies for industrial enterprises, financial structures and service organizations. This explains the high relevance of the development of new scientifically sound effective computational methods, algorithms and problem-oriented programs for testing web applications with a complex functional structure of internal and external interaction, which implement the capabilities of streaming data generated from the results of each of the test steps, and the application of the results in the process of managing the testing of web applications. The article describes the concept of modeling testing processes, research of the obtained models and development of analysis and prediction algorithms, based on a formalized apparatus of dynamic Bayesian networks. The Bayesian models proposed in the paper, built on the basis of statistical training, help to determine

time relationships for each of the parameters determined during the test procedure, provide the opportunity to predict test results by performing simulations using probabilistic inference methods.

***Keywords*:** web application vulnerabilities, Bayesian network, probabilistic inference problems, testing process, Monte Carlo method using Markov circuits, particle filtering algorithm.

For citation: Azarnova T.V., Polukhin P.V. Development of a concept and tools for modeling web application testing processes using fuzzing using dynamic Bayesian networks. *Modeling, Optimization and Information Technology*. 2023;11(4). URL: https://moitvivt.ru/ru/journal/pdf?id=1479 DOI: 10.26102/2310-6018/2023.43.4.031 (In Russ.).

Введение

Современное информационное обеспечение промышленности, бизнеса, финансовых структур, сферы образования и здравоохранения базируется в основном на веб-технологиях. Web-технологии построены на взаимодействии браузера и веб-сервера и обеспечивают важные преимущества как разработчикам, так и конечным пользователям. Разработчики создают кроссплатформенные приложения. Функции, выполняемые в оболочке веб-браузера, не зависят от операционной системы, предусмотрены инструменты непрерывного обновления и расширения возможностей приложений. Конечные пользователи избавлены от необходимости скачивать программы и обновления, привязанные к определенной операционной системе, поскольку приложения находятся на централизованном сервере, доступном по сети интернет. Наряду с весомыми преимуществами веб-приложения имеют серьезные недостатки, связанные с обеспечением информационной безопасности. Ежегодные статистические исследования в области информационной безопасности компаний Positive Technologies и MITRE, показывают, что высокий процент анализируемых веб-приложений содержат уязвимости различной степени критичности. Наличие уязвимостей связано как с ошибками разработчиков, которые стремятся добиться определенной функциональности и не уделяют должного внимания вопросам безопасности, так и с более глубокими причинами, связанными с развитием механизмов разработки веб-приложений.

Объединение в единую систему современных систем проектирования, разработки и взаимодействия отдельных компонентов web-приложений представляет собой унифицированную среду, предназначенную для решения различных прикладных задач. Элементы данной системы формируют единую программную экосистему, функционирующую и эволюционирующую в соответствии с предъявляемыми требованиями. В свою очередь, это приводит к появлению модулей и компонентов, которые не в полной мере согласуются с архитектурой самого приложения, что усложняет организацию взаимодействия между ними. Проблемы, связанные с уязвимостями веб-приложений, могут принести множество проблем, включая потерю персональных и финансовых данных, кражу парольно-адресной информации и нарушения доступа к приложению со стороны конечных пользователей.

Совокупность информационных систем и технологий, осуществляющих проектирование, создание, обновление и настройку взаимодействия Web-приложений представляет собой полноценную многокомпонентную, многофункциональную платформу. Компоненты данной системы непрерывно развиваются в соответствии с прогнозируемыми потребностями пользователей, темпы их развития носят несогласованный характер, нет единого механизма управления развитием платформы как единой системы с системными принципами взаимодействия. Проблемы, связанные с уязвимостями веб-приложений, могут нанести существенный вред как компаниям-владельцам веб-приложений, так и конечным пользователям. Некоторые уязвимости

допускают автоматическую эксплуатацию и способствуют массовому внедрению вредоносного кода в веб-ресурсы.

На сегодняшний день ученые и специалисты в области информационной безопасности ведут исследования по созданию современных методов и инструментальных средств тестирования, предназначенных для оптимизации механизмов поиска уязвимостей веб-приложений. Наибольшее применение в данной области находят средства математического моделирования на основе нейронных сетей, сетей Петри, конечных автоматов, нечетких множеств, компонентов имитационного и стохастического моделирования. В исследованиях Дж. Аррейнби и К. Имафидон [1] предложена модель нейронной сети, предназначенная для поиска программных ошибок в приложениях, и описан алгоритм ее внедрения в процесс безопасной разработки программного обеспечения. Нейросеть обучается на основе открытых баз уязвимостей программного обеспечения и позволяет находить участки приложения, в которых могут содержаться ошибки. А. Керамитис и С. Стольфо исследовали вопросы анализа сетевого траффика, обрабатываемого веб-приложениями, с целью разработки инструментов обнаружения различного рода ошибок. В ходе исследований учеными предложена математическая модель на основе Марковской цепи, позволяющая определить факт наличия индикаторов ошибок веб-приложений. В научных трудах П.Д. Зегжды и С.С. Корта [2] рассмотрен процесс появления аномалий в работе информационных систем в зависимости от различного набора входных данных. Это позволяет идентифицировать нормальное и некорректное поведение системы. В основу исследования авторами положен математический аппарат Марковских цепей, позволяющий представить процесс тестирования в виде дискретного или непрерывного стохастического процесса, позволяющего оценить вероятность перехода в новое состояние с учетом получения данных (свидетельств). Критерием отнесения поведения системы к аномальному является низкое значение переходной вероятности при переходе между двумя срезами Марковской цепи. Несмотря на значимость вопросов безопасности веб-приложений и большое количество исследований в данной области, на сегодняшний момент времени не разработан единый подход к комплексному обеспечению информационной безопасности в данной сфере.

Механизмы тестирования являются универсальным и достаточно апробированным инструментом поиска и выявления уязвимостей. На сегодняшний день выделяют тестирование на основе черного, белого и серого ящика. Каждый из методов реализует свой определенный набор механизмов для обнаружения ошибок веб-приложений. Фаззинг представляет собой разновидность тестирования и предназначен для поиска уязвимостей за счет случайного внесения изменений во входные параметры, участвующие в процедуре формирования результирующего запроса в веб-приложение [3]. По методикам анализа ошибок учеными выделяют мутационный и порождающий фаззинг, где формирование подходящих тестов происходит либо путем формирования случайной выборки, либо на основе внесения изменения в тесты, сформированные ранее. В рамках создания универсальных средств тестирования наиболее актуальным является комбинация различных подходов тестирования, в частности, объединение методов черного, белого и серого ящика [4]. Такой подход позволяет оптимизировать процедуры тестирования и снизить недостатки каждого из методов по отдельности. В рамках научного исследования рассматривается создание моделей и инструментальных средств для оптимизации процесса тестирования за счет применения динамических байесовских сетей (ДБС). Применение ДБС позволяет реализовать накопление результатов, осуществлять прогнозирование появления ошибок в новых состояниях, а также выявить ранее неизвестные уязвимости. Представлена концептуальная модель, позволяющая объединить методы фаззинга и модели тестирования на основе ДБС.

Материалы и методы

В рамках статьи представлена концептуальная модель процесса тестирования на основе ДБС, позволяющая поставить в соответствие каждому элементу тестирования его представление на основе семантической структуры ДБС и ее вероятностных распределений:

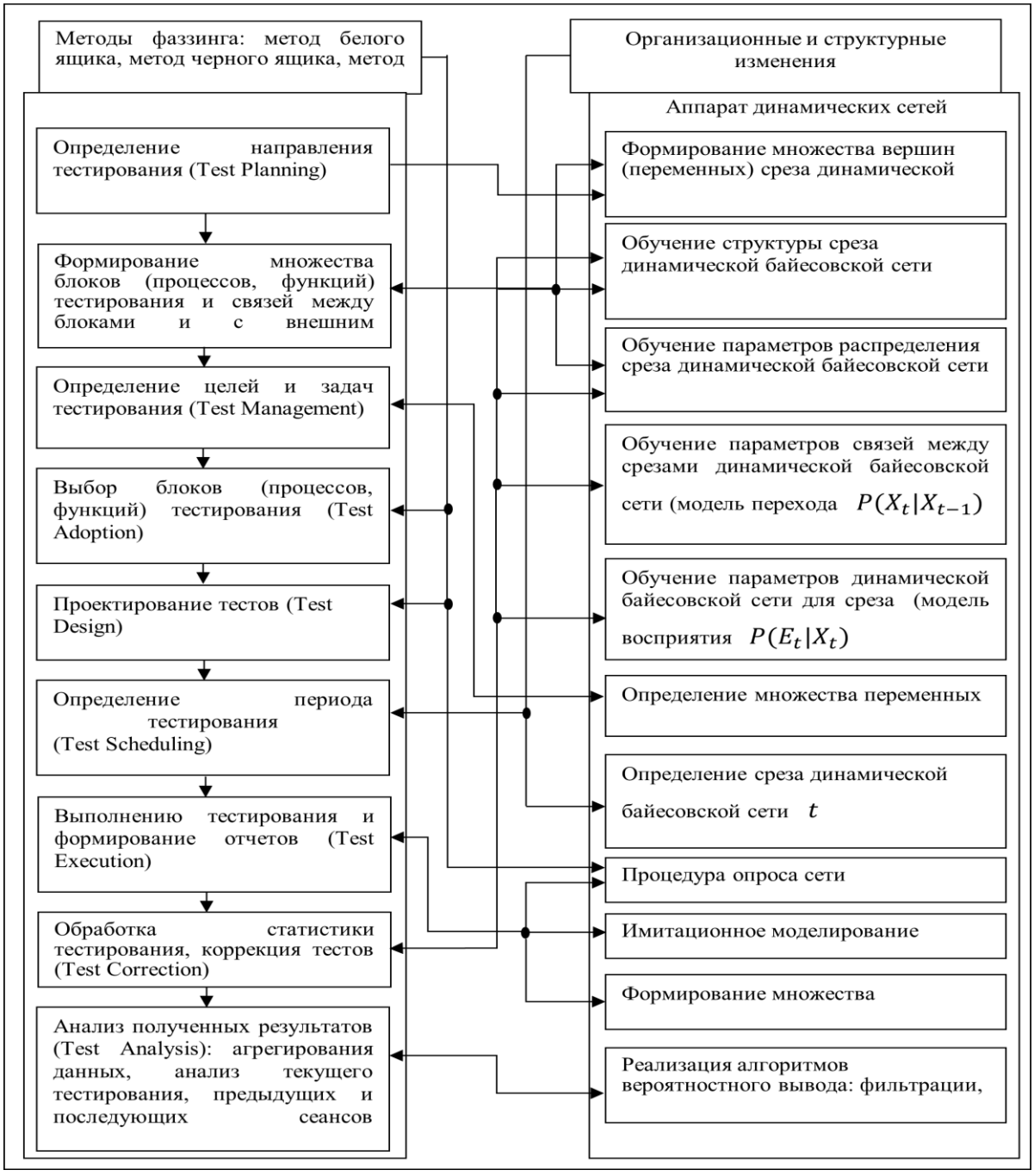

Рисунок 1 – Концептуальная модель фаззинга web-приложений на основе ДБС
Figure 1 – DBN-based web application phasing conceptual model

Байесовская сеть (БС) представляет собой направленный граф (НГА), содержащий переменные с дискретным или непрерывным вероятностным распределением величин. Вершина БС x может быть связана с одним или более

родительскими узлами $Parents(x)$. Если $Parents(x)=\varnothing$ считаем, что для вершины x выполняется критерий условной независимости. Распределение $P(x_i \mid Parents(x_i))$ формирует из таблицы условных вероятностей, задаваемой для переменной x с учетом ее множества родителей $Parents(x_i)$. Динамические вероятностные сети, в частности, ДБС могут рассматриваться в виде совокупности БС, развернутых на временном интервале $[t;t+k]$. В ДБС задаются вероятности перехода между временными срезами, а переменные структурно делятся на три основные категории: наблюдаемые, скрытые и свидетельства $Z_t=\{X_t,E_t,Y_t\}$ [5].

В рамках научного исследования каждому элементу концептуальной модели ставится в соответствие определенная модель тестирования, формализованная в виде переменных ДБС и имеющих связи в смежных временных срезах. Каждый временной срез представляет собой отдельный эксперимент по анализу определенных групп OWASP-ошибок, а узлы с временным состоянием определяют необходимые механизмы по настройке и корректировке модулей тестирования на каждом из срезов сети. Вероятностное распределение данных узлов соответствует марковскому процессу первого рода, что ограничивает возможность наличия связей переменных только в рамках двух смежных временных срезов. Данное условие гарантирует последовательное распространение свидетельств между срезами динамической байесовской сети.

Наибольший интерес, с точки зрения вероятностного моделирования процессов тестирования OWASP-ошибок, представляет группа ошибок, характеризующих процедуру обхода средств аутентификации и управления пользовательскими сессиями. Рассмотрим модель обнаружения данной группы ошибок на основе ДБС, состоящей из двух хронологических срезов. Расширенное описание функционального назначения узлов ДБС приведено в Таблице 1.

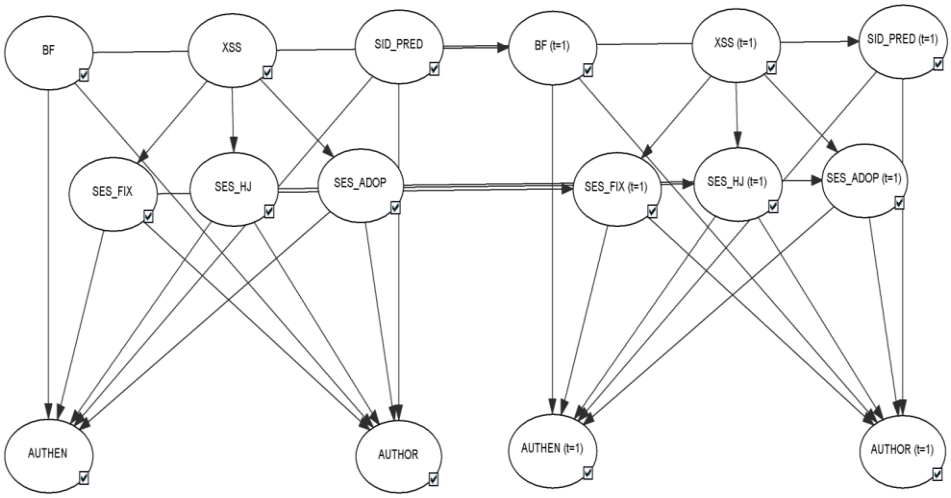

Рисунок 2 – Динамическая байесовская сеть тестирования уязвимостей средств аутентификации и управления пользовательскими сессиями
Figure 2 – Dynamic Bayesian vulnerability testing network for authentication and user session management

Таблица 1 – Характеристика узлов ДБС тестирования уязвимостей средств аутентификации и управления пользовательскими сессиями
Table 1 – Characteristics of DBN nodes for vulnerability testing of authentication tools and user session management

Название узла	Полное название узла	Характеристика
bf	CredentialsBruteForce_t	Реализация механизмов последовательного перебора параметров аутентификации веб-форм
xss	XSS_t	Реализация программной атаки типа «межсайтовый скриптинг»
ses_fix	SessionFixation_t	Атака на основе подбора или перехвата сессионного идентификатора
ses_hj	SessionHijack_t	Кража сессионного идентификатора
ses_adop	SessionAdoption_t	URL-фиксация сессионного идентификатора
sid_pred	SessionPrediction_t	Предсказания идентификатора сессии на основе общедоступных алгоритмов
author, authen	Authorization_t, Authentication_t	Атаки на аутентификацию, авторизацию пользователей приложения

Перехват учетных записей администраторов и супер-пользователей в большинстве случаев обладает наибольшей критичностью и приводит к утечке важных данных и компрометации целевой информационной системы. Элементы ДБС на Рисунке 1 представляют собой наборы программных компонентов, предназначенных для поиска определенного типа ошибки с учетом особенностей ее эксплуатации. В совокупности набор данных элементов представляет собой комплексный механизм по поиску уязвимостей, а ДБС устанавливает между ними вероятностные взаимосвязи с целью оптимизации процедуры обнаружения ошибок.

Процедура построения байесовской сети основывается на алгоритме Перла, представляющего собой циклическую операцию по добавлению ребер графа для текущей вершины с учетом условной независимости ее от родителей. В основе современных алгоритмов поиска оптимальной структуры ДБС используется объединение статистического подхода и метода на основе поиска максимума оценочной функции для каждой из вершин графа. Структурно данные алгоритмы можно разделить на два основных этапа. На первом этапе происходит формирование узлов-кандидатов либо в родительские вершины, либо в состав марковского покрытия. После чего производится оценка условной независимости текущей вершины по отношению к данным кандидатам. На следующем этапе происходит определение направленностей связи между вершинами за счет поиска экстремума оценочной функции. Производится циклическое вычисление оценок после выполнения операций добавления, удаления или изменения направления дуг графа.

Для поиска экстремума оценочной функции можно использовать следующие алгоритмы: поиск с восхождением к вершине и алгоритм имитации отжига. Второй алгоритм является более точным за счет того, что позволяет исключить образование локальных оптимумов [6]. В качестве основной оценки в данных алгоритма используется метрика Байеса-Дирихле.

С учетом семантических особенностей ДБС тестирования веб-приложений считаем, что переходные вероятности между срезами ДБС образуют Марковский процесс первого порядка [7]. Из этого следует, что $P\left(X_t|X_{0:t-1}\right)=P\left(X_t|X_{t-1}\right), P\left(E_t|X_{0:t},E_{0:t-1}\right)=P\left(E_t|X_t\right)$, а совместное распределение имеет

следующий вид:

$$P(X_0, X_1, \ldots, X_t, E_1, \ldots, E_t) = P(X_0)\prod_{i=1}^{t} P(X_i|X_{i-1})P(E_i|X_i), \quad (1)$$

где X_t, E_t – множество наблюдаемых переменных и переменных запроса , $P(X_0)$ – распределение вероятностей, соответствующее моменту времени t_0, $P(X_i|X_{i-1})$ – модель перехода из среза t_0 в t_1, $P(E_i|X_i)$ – модель восприятия.

Задачи тестирования на основе ДБС могут быть представлены в виде решения следующих основных задач вероятностного вывода: фильтрация, прогнозирование и сглаживание. Фильтрация реализуется за счет вычисления вероятностей $P(X_t|E_{1:t})$ при получении $E_{1:t}$ до среза t [8,9]:

$$\begin{aligned} &P(X_{t+1}|E_{1:t+1}) = P(X_{t+1}|E_{1:t}, E_{t+1}) = \alpha P(E_{t+1}|X_{t+1})P(X_{t+1}|E_{t:1}) = \\ &= \alpha P(E_{t+1}|X_{t+1})\sum_{X_t} P(X_{t+1}|X_t)P(X_t|E_{1:t}) \end{aligned} . \quad (2)$$

Предсказание позволяет вычислить вероятность $P(X_{t+k}|E_{1:t})$ для переменных ДБС для новых срезов $t+k+1$, если получены свидетельства к текущему моменту $t+k$:

$$P(X_{t+k+1}|E_{1:t}) = \sum_{X_{t+k}} P(X_{t+k+1}|X_t)P(X_{t+k}|E_{1:t}). \quad (3)$$

Сглаживание дает возможность вычисления $P(X_k|E_{1:t})$ и позволяет оценить все состояния переменных в прошлом при получении свидетельств до текущего момента включительно [10, 11]:

$$\begin{aligned} &P(X_k|E_{1:t}) = \alpha P(X_k|E_{1:k})P(E_{k+1:t}|X_k), \\ &P(E_{k+1:t}|X_k) = \sum_{X_{k+1}} P(E_{k+1:t}|X_k, X_{k+1})P(X_{k+1}|X_k). \\ &= \sum_{X_{k+1}} P(E_{k+1}|X_{k+1})P(E_{k+2:t}|X_{k+1})P(X_{k+1}|X_k) \end{aligned} \quad (4)$$

В рамках решения данных задач широко используются алгоритмы на основе метода Монте-Карло с применением цепей Маркова. Одним из таких алгоритмов является многочастичный фильтр (МЧФ). В основе алгоритма используется последовательное развертывание динамической байесовской сети на интервале $[t;t+k]$. На каждом срезе происходит распределение свидетельств и формирование выборок для каждой из переменных ДБС. После чего каждой из выборок ставится соответствующий вес с учетом связанных с переменной свидетельств. Формирование выборок производится в топологическом порядке, начиная с вершины графа и двигаясь к последнему узлу сети. Обобщенная структура алгоритма состоит из следующих шагов:

Шаг 1. Для среза $P(X_0)$ формируется N выборок.

Шаг 2. Определяются свидетельства для всех средой ДБС $E_1, E_2, ..., E_T$;

Шаг 3. Выполняется последовательный переход от среза t к $t+1$. Используя распределение $P(X_{t+1}|X_t)$ производится изменение выборок и расчет результирующего

распределения: $N\left(X_{t+1}\middle|E_{1:t}\right)=\sum_{X_t}P\left(X_{t+1}\middle|X_t\right)N\left(X_t\middle|E_{1:t}\right)$, $N\left(X_t\middle|E_{1:t}\right)$ – общее число выборок для X_t с учетом свидетельств $E_{1:t}$)→взвешиваются выборки с учетом новых свидетельств E_{t+1}, после чего для них задается вес $P\left(E_{t+1}\middle|\mathrm{X}_{t+1}\right)$→ определяется общий вес для каждой из выборок X_{t+1} с учетом свидетельств E_{t+1}: $W\left(X_{t+1}\middle|E_{1:t+1}\right)=P\left(E_{t+1}\middle|X_{t+1}\right)P\left(X_{t+1}\middle|E_{1:t}\right)$→веса, имеющие небольшие веса исключаются→ генерируются новые N выборок с учетом их весов.

Для оптимизации алгоритма МЧФ, а также снижения затрат на формирование большого числа выборок с целью получения наиболее точного распределения вероятностей будем использовать теорему Рао-Блэквелла-Колмогорова (РБК). Данная теорема позволяет улучшить статические параметры МЧФ на основе применения теории достаточных статистик. Использование РБК наиболее актуально для ДБС со сложной топологией, когда формирование большого числа выборок становится затруднительно. Рассмотрим применение РБК для МЧФ. Для этого разделим все скрытые переменные X_t на U_t и V_t в соответствии со следующим распределением вероятностей [12]:

$$P\left(X_{t+1}|X_t\right)=P\left(U_{t+1}|V_{t:t+1},U_t\right)P\left(V_{t+1}|V_t\right). \quad (5)$$

Тогда теорема РБК может быть получена через неравенство дисперсий для весов полной и редуцированной выборок $W\left(V_{0:t+1},U_{0:t+1}\right),W\left(V_{0:t+1}^i\right)$:

$$\mathrm{D}\left(W\left(V_{0:t+1}\right)\right)\le\mathrm{D}\left(W\left(V_{0:t+1},U_{0:t+1}\right)\right). \quad (6)$$

Результаты и их обсуждение

В экспериментальной части исследования проведена практическая верификация разработанных моделей, методов и алгоритмов для решения задач тестирования веб-приложений методом фаззинга. В рамках создания макета произведено развертывание и настройка веб-серверов, серверов баз-данных и приложений. Для проведения эксперимента представлен набор инструментальных средств тестирования уязвимостей средств аутентификации и управления пользовательскими сессиями. В качестве протоколов сетевого взаимодействия используется стек http/https. Передача данных происходит в виде структурированных данных языков описания json, xml и html.

В рамках верификации особенностей применения математического аппарата ДБС для решения разнородных задач тестирования веб-приложений в работе представлены оригинальные авторские методики. Первая методика реализована в виде набора проблемно-ориентированных инструментальных средств, разработанных в рамках научного исследования, реализованных на основе вероятностных моделей ДБС, вторая методика – случайное тестирование на основе черного ящика.

В результате проведения эксперимента были получены оценки эффективности и правдоподобия для каждого из методов, а также проведено сравнение предложенного подхода на основе динамических сетей Байеса и метода черного ящика. Применение разработанного инструментария позволило адаптировать процесс тестирования к предсказанию возможных неустойчивых состояний веб-приложений и способствовало обнаружению аномального поведения приложения в будущем состоянии. Применение концепции параллельных операций позволило оптимизировать процедуры обучения и вероятностного вывода и представить процесс тестирования в виде непрерывного,

высокопроизводительного процесса, объединяющего в себя функции самообучения и коррекции.

Таблица 2 – Сравнение результатов фаззинга на основе и существующих средств анализа ошибок
Table 2 – Fuzzing results comparison for existing tools of error analyses

№ п/п	Инструмент тестирования	Обнаруженные ошибки	Ложные срабатывания	Пропущено ошибок	Аномальные ошибки
1.	Acunetix	75	8	15	3
2.	Nessus	60	17	20	1
3.	OWASP ZAP	62	21	12	0
4.	Arachi	54	14	26	0
5.	Paros	50	22	29	0
6.	Burp Suite Pro	65	10	38	0
7.	W9scan	45	32	32	0
8.	Разработанный фаззер	80	2	4	10

Из Таблицы 2 видно, что разработанный фаззер на основе модели ДБС позволил выявить 10 аномальных ошибок на основе вероятностного вывода и выдачи качественных прогнозов относительно присутствия определенных программных ошибок в будущих состояниях веб-приложений. Такой подход позволяет выработать ряд мер по своевременной локализации ошибок и исключения возможных векторов атак.

Заключение

Приведенный в рамках исследования набор инструментов тестирования программ может быть применен для анализа и поиска сложных уязвимостей, связанных с аутентификацией и управлением сессиями, может быть легко использован в качестве составного элемента построения комплексной системы защиты веб-приложений, межсетевых экранов и фильтров безопасности. Развитие инструментальных средств на основе моделей ДБС показало свою состоятельность и позволило выявить множество аномальных ошибок на основе реализации процедуры вероятностного вывода. Для решения задач вероятностного вывода реализована возможность оценки генерируемых выборок за счет реализации ретроспективного анализа и своевременной коррекции формируемых выборок на основе алгоритма МЧФ.

Применение статистических алгоритмов в процессе обучения и вероятностного вывода ДБС позволяет оптимизировать процедуры получения оптимальной структуры, выработать подходы к оптимизации алгоритмов логического вывода и снизить временные затраты на реализацию процедур фаззинга.

Расширенное использование большого спектра серверов баз-данных и приложений позволяет получить максимальный охват наиболее распространенных ошибок аутентификации, выработать единый подход к их локализации и исключить возможность использования данных ошибок в процессе проведения атак на информационные системы, построенные на основе веб-приложений. Использование различных форматов передачи данных дает возможность анализа всех имеющихся типов

приложений, используемых для построения современных систем как на основе классических пользовательских приложений, так и на основе распространенных веб-сервисов REST и SOAP.

СПИСОК ИСТОЧНИКОВ

1. Adebiyi A.A., Arreymbi J., Imafidon C. Neural network based security tool for analyzing software. *Advances in Information and Communication Technology*. 2013;80–87.
2. Zegzhda P.D., Kort S.S., Suprun A.F. Detection of anomalies in behavior of the software with usage of Markov chains. *Automatic Control and Computer Sciences*. 2015;820–825.
3. Котенко И.В., Чичулин А.В. Применение графов атак для оценки защищенности компьютерных сетей и анализа событий безопасности. *Системы высокой доступности*. 2013;103–110.
4. Бейзер Б. *Тестирование черного ящика*. СПб.: Питер; 2004. 321 с.
5. Korb K.B., A.E. Nicholson. *Bayesian Artificial Intelligence*. Boca Raton, CRC Press; 2004. 491 p.
6. Полухин П.В. Инструменты оптимизации многочастичного фильтра для вероятностных моделей динамических систем. *Системы управления и информационные технологии.* 2021;4–10.
7. Chickering D.M. Optimal Structure Identification with Greedy Search. *Journal of Machine Learning Research*. 2002;507–554.
8. Pearl J. *Causality: Models, Reasoning and Inference*. N.Y.: Cambridge University Press; 2009. 484 p.
9. Тулупьев А.Л., Сироткин А.В., Николенко С.И. *Байесовские сети логико-вероятностный подход*. СПб.: Издательство СПБГУ; 2009. 400 с.
10. Koller D, Friedman N. *Probabilistic graphical models. Principles and Techniques.* Cambridge, MIT Press; 2009.1231 p.
11. Russel S., Norvig P. *Artificial intelligence a modern approach*. N.J.: Pearson; 2009. 484 p.
12. Леман Э. *Проверка статистических гипотез*. М.: Наука; 1987. 408 с.

REFERENCES

1. Adebiyi A.A., Arreymbi J., Imafidon C. Neural network based security tool for analyzing software. *Advances in Information and Communication Technology*. 2013;80–87.
2. Zegzhda P.D., Kort S.S., Suprun A.F. Detection of anomalies in behavior of the software with usage of Markov chains *Automatic Control and Computer Sciences*. 2015;820–825.
3. Kotenko I.V., Chichulin A.V. Primenenie grafov atak dlya ocenki zaschischennosti kompyuternyh setej i analiza sobytij bezopasnosti. *Sistemy vysokoj dostupnosti*. 2013;103–110. (In Russ.).
4. Beizer B. *Black Box testing*. Spb, Piter; 2004. 321 p. (In Russ.).
5. Korb K.B., Nicholson A.E. *Bayesian Artificial Intelligence*. Boca Raton, CRC Press; 2004. 491 p.
6. Polukhin P.V. Instrumenty optimizacii mnogochastichnogo filtra dlya veroyatnostnyh modelej dinamicheskih sistem. *Sistemy upravleniya i informacionnye tehnologii*. 2021;4–10. (In Russ).
7. Chickering D.M. Optimal structure identification with greedy search. *Journal of Machine Learning Research*. 2002;507–554.
8. Pearl J. *Causality: Models, Reasoning and Inference*. N.Y., Cambridge University Press; 2009. 484 p.
9. Tulupev A.L., Sirotkin A.V., Nikolenko S.I. *Bajesovskie seti logiko-veroyatnostnyj*

podhod. Saint Petersburgh, Izdatelstvo SPBGU; 2009. 400 p. (In Russ).
10. Koller D., Friedman N. *Probabilistic graphical models. Principles and Techniques*. Cambridge, MIT Press; 2009. 1231 p.
11. Russel S., Norvig P. *Artificial intelligence a modern approach*. N.J., Pearson; 2009. 484 p.
12. Lemain E. *Proverka statisticheskih gipotez*. Moscow, Nauka; 1987. 408 p. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Азарнова Татьяна Васильевна, доктор технических наук, заведующий кафедрой математических методов исследования операций факультета прикладной математики, информатики и механики Воронежского государственного университета, Воронеж, Российская Федерация.
e-mail: ivdas92@mail.ru

Tatyana V. Azarnova, Doctor of Technical Sciences, Head of Department of Mathematical Methods of Operations Research, Faculty of Applied Mathematics, Voronezh State University, Voronezh, the Russian Federation**.**

Полухин Павел Валерьевич, кандидат техн. наук, кафедра математических методов исследования операций факультета прикладной математики, информатики и механики Воронежского государственного университета, Воронеж, Российская Федерация.
e-mail: alfa_force@bk.ru

Pavel V. Polukhin, Candidate of Technical Sciences, Department of Mathematical Methods Operations Research, Faculty of Applied Mathematics, Informatics and Mechanics, Voronezh State University, Voronezh, the Russian Federation.

Статья поступила в редакцию 24.11.2023; одобрена после рецензирования 11.12.2023; принята к публикации 22.12.2023.

The article was submitted 24.11.2023; approved after reviewing 11.12.2023; accepted for publication 22.12.2023.