МОДЕЛЬ ПРОЦЕССА ФУНКЦИОНИРОВАНИЯ И АЛГОРИТМ ОПРЕДЕЛЕНИЯ ОПТИМАЛЬНЫХ ЗНАЧЕНИЙ КОНФИГУРИРУЕМЫХ ПАРАМЕТРОВ ВЕБ-СЛУЖБЫ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Каверин С. С.[1], Максимов Р. В.[2], Москвин А. А.[3]

DOI: 10.21681/2311-3456-2025-1-50-62

Цель исследования: *повышение защищенности веб-службы корпоративных информационных систем в условиях сетевой разведки.*

Используемые методы: *оптимизации по Парето, идеальной точки, Нелдера-Мида, роя частиц, имитации отжига.*

Результат исследования: *разработана модель функционирования веб-службы корпоративных информационных систем в условиях сетевой разведки, которая реализована в виде полумарковского случайного процесса с дискретными состояниями и непрерывным временем. Получены вероятностно-временные характеристики исследуемых процессов, которые необходимы для определения оптимального режима конфигурирования параметров веб-службы.*

Решена задача векторной оптимизации для определения оптимальных значений параметров веб-службы корпоративных информационных систем, таких как количество фрагментов HTTP-ответа, время между этими фрагментами, а также количество ложных веб-серверов, позволяющих максимизировать результативность защиты веб-службы корпоративных информационных систем и минимизировать вероятность отказа ложных веб-серверов при соответствующих ограничениях.

Научная новизна: *заключается в разработке модели и алгоритма поиска оптимальных параметров веб-службы корпоративных информационных систем в условиях сетевой разведки с применением математического аппарата полумарковских случайных процессов и скаляризацией задачи векторной оптимизации методом идеальной точки.*

Ключевые слова: *случайный процесс, вероятностно-временные характеристики, веб-ресурсы, метод идеальной точки, веб-сессия, интервально-переходные вероятности, сетевая разведка.*

Введение

В условиях активной внешнеполитической деятельности нашей страны наблюдается заметный рост числа кибератак на веб-службы. Общие тенденции в кибербезопасности показывают, что такие порталы, как «Госуслуги», «Личный кабинет ПФР», где обрабатывается большое количество персональных данных, остаются основными целями для кибератак, таких как фишинг, атаки на учетные записи и компрометация данных. Проблемы, связанные со взломом паролей, подстановкой учетных данных и использованием словарных атак, стали одними из ключевых в сфере кибербезопасности. Атаки, направленные на взлом учетных записей, представляют существенную угрозу для пользователей и организаций, часто вызывая значительные финансовые потери и ущерб репутации. Даже несмотря на применяемые средства защиты, ввиду использования импортного оборудования, а также сетей связи общего пользования и недостаточной степени доверия к открытому программному обеспечению, данные угрозы остаются актуальными [1]. Веб-службы делятся на несколько типов в зависимости от их назначения и архитектуры:

1. RESTful веб-службы. Используют протокол HTTP для обмена данными. Основаны на стандартах и предоставляют доступ через URL.
2. SOAP веб-службы. Имеют более сложную структуру, используют XML для передачи данных. Поддерживают сложные сценарии взаимодействия.
3. GraphQL веб-службы. Современные API, позволяющие клиенту запрашивать данные, определяя их структуру.
4. RPC (Remote Procedure Call). Позволяют удалённый вызов процедур.

1 Каверин Сергей Сергеевич, адъюнкт, Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С. М. Штеменко, г. Краснодар, Россия. E-mail: sergey_kav995@mail.ru

2 Максимов Роман Викторович, доктор технических наук, профессор, Заслуженный изобретатель Российской Федерации, Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С. М. Штеменко, г. Краснодар, Россия. E-mail: rvmaxim@yandex.ru

3 Москвин Артем Александрович, кандидат технических наук, Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С. М. Штеменко, г. Краснодар, Россия. E-mail: tema.kg9012@gmail.com

К основным типам атак на веб-службы относятся следующие.

1. DDoS-атаки. Наблюдался рост сложности и частоты атак типа DDoS (Distributed Denial of Service), направленных на веб-приложения и API. В частности, Cloudflare[4] сообщила о 466% росте атак на отдельные страны и индустрии, такие как игры и IT-компании, что обусловлено как политическими мотивами, так и финансовыми интересами злоумышленников.
2. Атаки на API. Около 60% динамического трафика веб-приложений связано с API, что делает их привлекательной целью для атак. Исследования показывают, что многие компании не осознают масштаба своего API-трафика, и около четверти API являются «теневыми», что создает дополнительные риски.
3. Боты и автоматизация атак. Около 31% всего веб-трафика приходится на боты, из которых 93% считаются потенциально вредоносными. Они используются для различных атак, включая кражу учетных данных, инвентаризацию сайтов и проведение атак на доступность.
4. Уязвимости веб-приложений. Отчет от Edgescan[5] показал, что среднее время на устранение критических уязвимостей увеличилось, что создает длительные окна для злоумышленников. Основными уязвимостями остаются SQL-инъекции, XSS (межсайтовый скриптинг) и атаки на авторизацию.
5. Фишинг и социальная инженерия. По данным на 2024 год, 96% фишинговых атак распространяются через email, и эти атаки стали основным методом для получения доступа к веб-приложениям и учетным записям пользователей. Атаки на компании с использованием фишинга остаются основной угрозой для бизнеса.

Все эти атаки особенно опасны в условиях, когда многие пользователи продолжают использовать простые и легко угадываемые пароли. Кроме того, тенденция к повторному использованию паролей на различных веб-ресурсах делает успешную атаку на один ресурс потенциальной угрозой для всех остальных, где используются те же учетные данные.

Ключевым этапом подготовки компьютерных атак является сетевая разведка, цель которой – сбор информации о составе, структуре, алгоритмах работы, местоположении и принадлежности компонентов веб-системы, а также анализ обрабатываемых и хранимых данных. Этот процесс необходим для выявления потенциальных целей, уязвимостей и централизации усилий при осуществлении атак или других вредоносных воздействий.

Анализ публикаций [2–5] в сфере противодействия сетевой разведке показывает, что активно развиваются технологии как для защиты информационных систем от исследуемых угроз, так и для реализации сетевой разведки и компьютерных атак. Например, в контексте веб-службы защита от таких методов, как подбор паролей по словарю и подстановка учетных данных с целью обеспечения конфиденциальности и целостности данных, реализуется через использование сложных паролей, блокировки учетных записей, многофакторной аутентификации и ограничений на частоту запросов.

С другой стороны, методы атак на персональные данные со стороны злоумышленников продолжают совершенствоваться, что затрудняет обеспечение должной защиты веб-службы корпоративных информационных систем. В то же время, возможности протоколов, поддерживающих работу этой веб-службы, позволяют конфигурировать параметры с использованием сетевых «ловушек» (network tarpits) [6–8] и обманных систем (deception systems). Сетевые ловушки — это технологии или подходы, используемые для обмана, замедления или анализа действий злоумышленников, взаимодействующих с веб-службой. Эти ловушки имитируют работу системы, создавая иллюзию нормального функционирования, но при этом затрудняют или делают бесполезными попытки атак. Основная цель – защитить основные ресурсы системы, снизить эффективность атаки и собрать информацию о методах злоумышленника. В контексте защиты веб-службы использование таких технологий, как сетевые «ловушки», может быть следующим:

1. Замедление атак. Сетевая ловушка искусственно увеличивает время отклика сервера для подозрительных запросов. Это особенно эффективно против автоматизированных атак, таких как brute force или DDoS.
2. Обман злоумышленников. Создание фальшивых веб-серверов или API-методов для введения, атакующих в заблуждение. Например, злоумышленник взаимодействует с фальшивой системой, расходуя ресурсы на бесполезные действия, и вместо настоящих данных сервера получает поддельные ответы.
3. Снижение эффективности сканирования. Сетевые ловушки замедляют работу автоматизированных инструментов, таких как сканеры уязвимостей, за счёт имитации «медленных» соединений.
4. Анализ атак. Сетевые ловушки могут собирать данные о действиях злоумышленников, предоставляя администраторам информацию о потенциальных векторах атак.

4 Отчет по кибератакам на веб-приложения от Cloudflare, URL: https://newsletter.radensa.ru/wp-content/uploads/2024/10/BDES-5907_State-of-App-Security-2024.pdf

5 Отчет по уязвимостям веб-приложений от Edgescan, URL: https://info.edgescan.com/hubfs/23DOWNLOADABLE%20CONTENT/Vulnerability%20Statistics%20Reports/Edgescan_VulnerabilityStatsReport2024.pdf

5. Перенаправление атак. Сетевые ловушки могут перенаправлять избыточный трафик на фальшивые ресурсы, предотвращая перегрузку основных серверов.

Веб-система представляет собой интегрированное программное решение, включающее в себя веб-клиентов, веб-серверы, базы данных, приложения для обработки бизнес-логики, пользовательские интерфейсы и средства обеспечения безопасности. Ее архитектура основана на клиент-серверной модели, что позволяет эффективно распределять ресурсы и централизованно управлять данными. Веб-система работает в рамках стека сетевых протоколов TCP/IP. Обмен информацией между веб-клиентами и веб-серверами осуществляется через протокол прикладного уровня HTTP в модели OSI, предназначенный для передачи гипертекстовых документов по сети, в частности, через интернет. Протокол HTTP описывается в нескольких RFC (Request for Comments), в том числе:

1. RFC 2616 – «Hypertext Transfer Protocol – HTTP/1.1». Этот RFC был основным для HTTP/1.1, и в нем подробно описаны все аспекты работы протокола: методы, структура сообщений, коды состояния, заголовки, кэширование и другие.
2. RFC 7230-7235 – «Hypertext Transfer Protocol (HTTP/1.1)». В 2014 году был выпущен набор из шести документов, который обновил и уточнил спецификации, содержащиеся в RFC 2616. Эти документы описывают HTTP/1.1 и более детально регламентируют все аспекты протокола.
3. RFC 7540 – «HTTP/2». Этот RFC описывает протокол HTTP/2, который улучшает производительность за счет использования бинарных фреймов и мультиплексирования запросов.
4. RFC 9000 – «QUIC: A UDP-based Multiplexed and Secure Transport». RFC 9000 описывает HTTP/3, который использует протокол QUIC для повышения скорости и безопасности соединений.

После установления коммуникационного канала и согласования параметров веб-клиент инициирует веб-сессию, отправляя последовательность запросов к веб-серверу для получения необходимых веб-ресурсов, на которые веб-сервер, в свою очередь, отвечает.

Веб-клиент устанавливает соединение (чаще всего через веб-браузер) с веб-сервером через порт 80 для HTTP или 443 для HTTPS, он отправляет запрос, включающий метод (например, GET или POST), URL запрашиваемого ресурса, версию протокола HTTP и дополнительные заголовки, если это необходимо. Следующим шагом является обработка сервером этого запроса. Он может включать в себя обращение к базе данных, выполнение серверного скрипта или просто выборку статического файла. Далее сервер отправляет ответ клиенту, который содержит статусный код (например, 200 для успешного запроса), версию протокола HTTP, заголовки ответа и тело сообщения (например, HTML-документ). Клиент получает ответ и обрабатывает его. Если это HTML-документ, браузер анализирует HTML, CSS, JavaScript, а затем отображает страницу пользователю. Последним этапом является закрытие соединения, которое происходит после завершения передачи данных. Каждый запрос в HTTP является отдельным и независимым. После завершения передачи данных соединение между клиентом и сервером закрывается. В отличие от других протоколов, таких как FTP, HTTP не требует постоянного поддержания соединения. Однако в HTTP/1.1 и более поздних версиях может использоваться постоянное соединение для отправки нескольких запросов через одно соединение. Диалог между клиентом и сервером осуществляется поэтапно: запрос – ответ – запрос. Исходя из этого управление процессом текущей веб-сессии может осуществляться через передачу сервером HTTP-ответа, разделенного на фрагменты d_1, d_2, ..., d_n, в ответ на запрос клиента. Передача данных осуществляется с изменяемыми интервалами времени T_1, T_2, ..., T_n, [2] как показано на рисунке 1.

Для исчерпания временного ресурса средств злоумышленника за счет имитации веб-сессии низкого качества, а также введения неопределенности посредством создания в сети ложных веб-серверов, необходимо разработать модель функционирования корпоративной сети передачи данных при конфигурировании параметров веб-службы и использовании ложных сетевых информационных объектов, а также алгоритма определения оптимальных значений этих параметров [9–11].

Модель функционирования корпоративной сети передачи данных при конфигурировании параметров веб-службы

Разработанная модель включает в себя два случайных процесса с дискретными состояниями, описывающими различные этапы работы HTTP-протокола.

С одной стороны, этапы жизненного цикла веб-службы (далее – система V), представлены как случайный процесс с дискретными состояниями и непрерывным временем. В качестве дискретных состояний выступают этапы функционирования системы V, а эволюция системы происходит под воздействием случайных событий, таких как получение и отправка HTTP-запросов.

С другой стороны, процесс функционирования ложных веб-серверов в условиях ведения сетевой разведки (далее – система D) может быть представлен в виде многоканальной системы массового обслуживания с отказами, в которую поступает поток

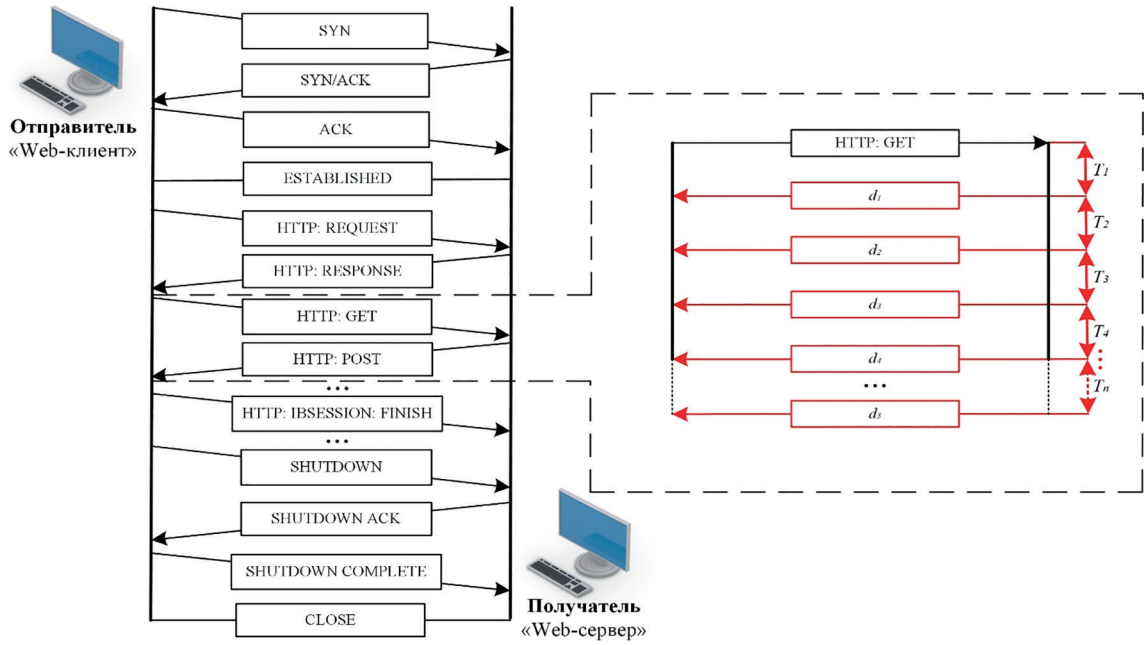

Рис. 1. Процесс установления веб-сессии HTTP и направления веб-сервером на поступивший от клиента HTTP-запрос последующего HTTP-ответа, разделенного на фрагменты d_1, d_2, ..., d_n через изменяемые интервалы времени T_1, T_2, ..., T_n

заявок на доступ к ложным веб-серверам. Число возможных состояний этого случайного процесса определяется количеством ложных веб-серверов.

Основные вероятностные характеристики полумарковского процесса включают в себя: функцию распределения времени ожидания перехода из состояния i в состояние j (далее – $F_{ij}(t)$), и вероятности этого перехода (далее – p_{ij}). На рисунке 2 представлен ориентированный граф случайного процесса для системы V, в таблице 1 описаны его дискретные состояния, а в таблице 2 содержатся вероятностные характеристики.

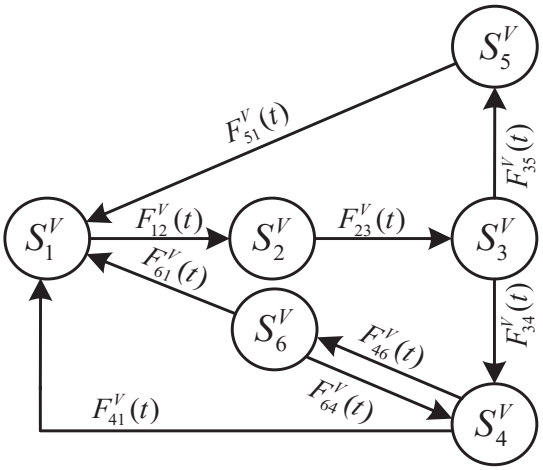

Рис. 2. Граф состояний системы V

Предположим, что вероятностные характеристики исследуемых процессов, в силу выполнения свойств простейшего потока, подчиняются экспоненциальному закону распределения [12]:

$$F_{ij}(t) = 1 - e^{-\lambda_{ij} t}, \quad (1)$$

$$p_{ij} = \int_0^\infty f_{ij}(t) \prod_{k=1,k\neq j}^{n} (1 - F_{ik}(t))\, dt, \quad (2)$$

где: λ_{ij} – интенсивности потока событий, которые переводят исследуемые системы из состояния i в состояние j, $f_{ij}(t)$ – функция плотности распределения времени ожидания перехода из состояния i в состояние j. На рисунке 3 представлен ориентированный граф случайного процесса для системы D, таблице 3 содержит описание его дискретных состояний, а в таблице 4 приведены вероятностные характеристики.

Система D содержит n ложных веб-серверов и является многоканальной системой массового обслуживания с отказами. В систему поступает один тип заявок (поток является однородным). Все ложные веб-серверы идентичны, следовательно, любая заявка может быть обработана любым ложным веб-сервером за одинаковое случайное время. Заявки, поступающие в систему D, образуют простейший поток с интенсивностью подключений сетевой разведки (network reconnaissance) λnr. Время обслуживания заявок на любом из ложных веб-серверов подчиняется экспоненциальному закону с интенсивностью:

$$\mu = \frac{n_{ch}}{d \cdot T_{res}}, \quad (3)$$

где: d – количество фрагментов, на которые разделен HTTP-ответ, T_{res} – время между фрагментами HTTP-ответа, n_{ch} – количество возможных активных

Таблица 1.

Дискретные состояния системы V

Дискретные состояния	Описание состояний
S_1^V	ожидание сервером поступления от клиента (нарушителя) на порт 80 TCP пакетов с флагом SYN на установление сетевого соединения (клиент (нарушитель) и веб-сервер находятся в состоянии простоя)
S_2^V	ожидание веб-сервером поступления от клиента (нарушителя) HTTP-запроса с методом GET на предоставление запрашиваемого веб-ресурса
S_3^V	ожидание клиентом поступления от веб-сервера HTTP-ответа об успешной авторизации с кодом состояния 200 OK и установления легитимной веб-сессии или ожидание нарушителем перенаправления его на ложный веб-сервер после 3 неудачных попыток авторизации
S_4^V	ожидание нарушителем после очередной попытки авторизации окончания поступления от ложного веб-сервера множества промежуточных откликов, разделенных на фрагменты, направляемые через изменяемые интервалы времени или окончания веб-сессии между нарушителем и ложным веб-сервером
S_5^V	ожидание окончания веб-сессии между клиентом и веб-сервером
S_6^V	ожидание очередной попытки нарушителя авторизоваться на ложном веб-сервере

Таблица 2.

Вероятностные характеристики процесса функционирования системы V

Переменная	Описание вероятностных характеристик
$F_{12}^V(t)$	функция распределения времени ожидания веб-сервером поступления от клиента (нарушителя) на порт 80 TCP пакетов с флагом SYN на установление сетевого соединения
$F_{23}^V(t)$	функция распределения времени ожидания веб-сервером поступления от клиента (нарушителя) HTTP-запроса с методом GET на аутентификацию в запрашиваемом веб-ресурсе
$F_{34}^V(t)$	функция распределения времени ожидания нарушителем перенаправления его на ложный веб-сервер после 3 неудачных попыток авторизации
$F_{35}^V(t)$	функция распределения времени ожидания клиентом поступления от сервера HTTP-ответа об успешной авторизации клиента с кодом состояния 200 OK и установления легитимной веб-сессии
$F_{41}^V(t)$	функция распределения времени ожидания окончания информационного обмена между нарушителем и веб-сервером
$F_{46}^V(t)$	функция распределения времени ожидания нарушителем окончания поступления от ложного веб-сервера множества промежуточных откликов, разделенных на фрагменты, направляемые через изменяемые интервалы времени с кодом состояния 401 UNAUTHORIZED после очередной попытки авторизации
$F_{51}^V(t)$	функция распределения времени ожидания окончания информационного обмена между клиентом и веб-сервером
$F_{61}^V(t)$	функция распределения времени ожидания окончания информационного обмена между нарушителем и ложным веб-сервером
$F_{64}^V(t)$	функция распределения времени ожидания очередной попытки нарушителя авторизоваться на ложном веб-сервере

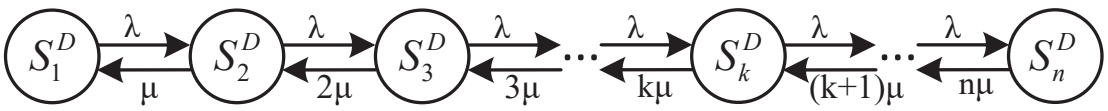

Рис.3. Граф состояний системы D

Таблица 3.

Дискретные состояния системы D

Дискретные состояния	Описание состояний
S_1^D	ожидание первым ложным веб-сервером подключения нарушителя, состояние простоя
S_2^D	ожидание вторым ложным веб-сервером подключения нарушителя, в системе находится 1 заявка, один ложный веб-сервер занят, остальные простаивают
S_3^D	ожидание третьим ложным веб-сервером подключения нарушителя, в системе находится 2 заявки, два ложных веб-сервера заняты, остальные простаивают
S_k^D	ожидание k-м ложным веб-сервером подключения нарушителя, в системе находится $k-1$ заявок, $k-1$ ложных веб-серверов заняты, остальные простаивают
S_n^D	ожидание отказа системы в обслуживании нарушителя, все веб-серверы заняты

Таблица 2.

Вероятностные характеристики процесса функционирования системы D

Переменная	Описание вероятностных характеристик
$F_{12}^D(t)$	функция распределения времени ожидания первым ложным веб-сервером подключения нарушителя
$F_{23}^D(t)$	функция распределения времени ожидания вторым ложным веб-сервером подключения нарушителя
$F_{(k-1)k}^D(t)$	функция распределения времени ожидания k-м ложным веб-сервером подключения нарушителя
$F_{(n-1)n}^D(t)$	функция распределения времени ожидания n-м ложным веб-сервером подключения нарушителя

веб-сессий на одном ложном веб-сервере, λ_{nr} – интенсивность подключений сетевой разведки.

В любой момент времени может произойти лишь одно из двух событий, которые приводят к изменению состояния системы D. Поступление заявки в систему осуществляется с интенсивностью подключений сетевой разведки λ_{nr}, k – это количество заявок. Если случайный процесс находится в состоянии S_k^D, при котором $k < n$, то происходит переход в состояние S_{k+1}^D (начало обслуживания поступившей заявки на одном из свободных ложных веб-серверов), а интенсивность перехода равна λ_{nr}. Если же случайный процесс находится в состоянии S_n^D, когда все ложные веб-серверы заняты обслуживанием заявок, то состояние S_n^D случайного процесса остается неизменным, что эквивалентно отказу в обслуживании поступившей заявки. Таким образом, переход из состояния S_k^D в состояние S_{k+1}^D, при котором $k < n$ происходит с интенсивностью λ_{nr}, а завершение обслуживания заявки на одном из ложных веб-серверов происходит с интенсивностью μ.

Математическая модель исследуемых систем может быть представлена как отображение множества входных параметров модели (множество Z) во множество выходных вероятностно-временных характеристик (множество Y):

$$Z^V \rightarrow Y^V, Z^V = \{S^V, A^V, X^V\};\ Y^V = \{P^V, G^V\}, \quad (4)$$

$$Z^D \rightarrow Y^D, Z^D = \{S^D, A^D, X^D\};\ Y^D = \{P^D, G^D\}, \quad (5)$$

где S^V, S^D – множества дискретных состояний систем S, D; A^V, A^D – множества неуправляемых факторов систем S, D; X^V, X^D – множества управляемых факторов систем S, D; $P^V = \{P_{ij}^V(t)\}$, $P^D = \{P_{ij}^D(t)\}$ – множества интервально-переходных вероятностей пребывания систем S, D в состоянии j из состояния i в момент времени t; $G^V = \{G_{ij}^V(t)\}$, $G^D = \{G_{ij}^D(t)\}$ – множества вероятностей первого достижения состояния j из состояния i к моменту времени t для систем S, D.

Неуправляемыми и управляемыми факторами для рассматриваемых систем являются:

$$A^V = \{F_{12}^V(t), F_{23}^V(t), F_{34}^V(t), F_{35}^V(t), F_{51}^V(t), F_{46}^V(t), F_{61}^V(t)\}, \quad (6)$$

$$A^D = \{\lambda_{nr}, n_{ch}\}, \quad (7)$$

$$X^V = \{F_{46}^V(t)\}, \text{ при } \lambda_{46}^V = \frac{n}{d \cdot T_{res}}, \quad (8)$$

$$X^D = \{d, T_{res}, n\}, \text{ при } \mu_1^D = \frac{n_{ch}}{d \cdot T_{res}}, \mu_2^D = \frac{2n_{ch}}{d \cdot T_{res}}, \ldots, \mu_n^D = \frac{nn_{ch}}{d \cdot T_{res}}, \quad (9)$$

где n – количество ложных веб-серверов.

Для нахождения интервально-переходных вероятностей $P_{ij}(t)$ используется решение системы интегральных уравнений вида (10):

$$P_{ij}(t) = \delta_{ij}\,\Psi_i(t) + \sum_{k=1}^{n} p_{ik} \int_0^t f_{ik}(t) P_{kj}(t-\tau)\,d\tau, \qquad (10)$$

$$\Psi_i(t) = 1 - \sum_{j=1}^{n} p_{ij}\,F_{ij}(t). \qquad (11)$$

Процесс решения таких интегральных уравнений подробно изложен в [13], и в матричной форме он будет выглядеть следующим образом:

$$P(t) = \pounds^{-1}\{[I - p \times f(s)]^{-1}\,\Psi(s)\}. \qquad (12)$$

На рисунках 4 и 5 представлены результаты расчетов вероятностно-временных характеристик веб-сессий, функционирующих в одинаковых внешних условиях, но при различных значениях параметров веб-службы, которые свидетельствуют о том, что наилучшие значения для системы S, являются наихудшими для системы D.

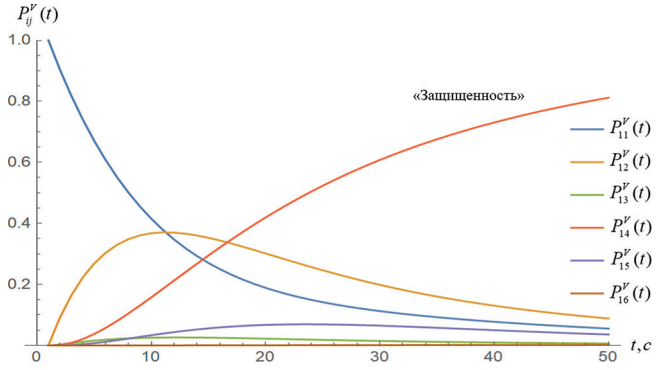

Рис. 4. Результаты расчетов интервально-переходных вероятностей нахождения системы S в состоянии j из состояния i к моменту времени t для процесса функционирования веб-службы с использованием конфигурирования параметров веб-сессии

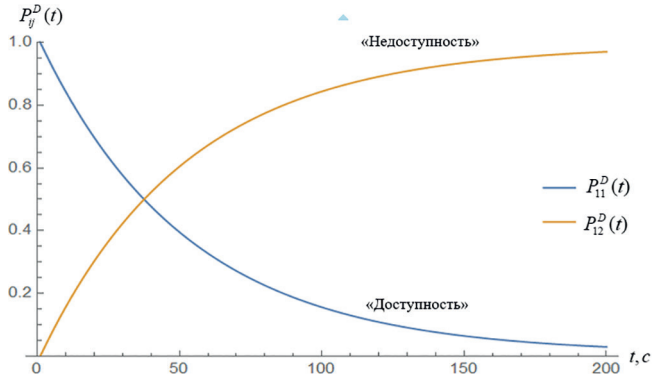

Рис. 5. Результаты расчетов интервально-переходных вероятностей нахождения системы D в состоянии j из состояния i к моменту времени t для процесса функционирования веб-службы с использованием конфигурирования параметров веб-сессии

Функции распределения Gij(t) находятся из следующего выражения:

$$G(t) = \pounds^{-1}\{s^{-1} \cdot p \cdot f(s) \cdot (I - p \cdot f(s))^{-1} \cdot \cdot [\mathrm{I} \times (I - p \cdot f(s))^{-1}]^{-1}\}. \qquad (13)$$

Функции $G_{ij}(t)$ позволяют оценить вероятности достижения соответствующих состояний впервые к конкретному моменту времени. На рисунке 6 изображен случай с обслуживанием нелегитимных клиентов, показывающий длительность первого посещения системой некоторых состояний с определенной вероятностью.

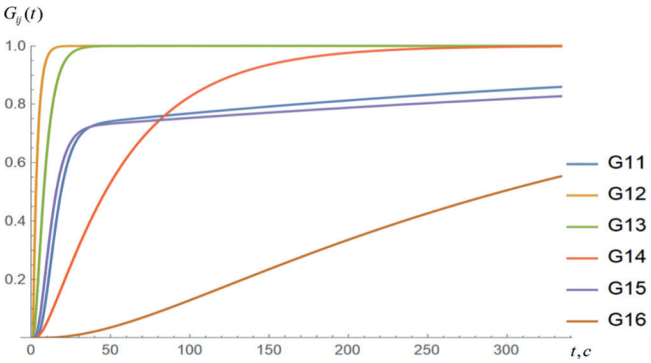

Рис. 6. Функции распределения $G_{ij}(t)$ времени первого посещения состояний процесса для процесса функционирования веб-службы с использованием конфигурирования параметров HTTP-ответа

Конфигурирование параметров веб-службы корпоративных информационных систем повышает вероятность нахождения нарушителя в состоянии удержания, однако при этих же параметрах понижается вероятность доступности ложных веб-серверов, что, в свою очередь, приводит к снижению вероятности нахождения системы в состоянии информационного обмена. Таким образом, возникает задача оптимизации конфигурируемых параметров веб-службы корпоративных информационных систем, при которой ложные веб-серверы будут функционировать наиболее эффективно с точки зрения критериев «доступности» и «защищенности».

Алгоритм определения оптимальных значений параметров конфигурирования веб-службы

Для нахождения оптимальных значений параметров веб-службы, при которых защищенность корпоративной информационной системы будет максимальной, а вероятность отказа ложных веб-серверов будет минимальной, разработан соответствующий алгоритм, который поясняется псевдокодом последовательности действий, представленном на рисунке 7.

Исходные данные для данного алгоритма указаны в таблице 5.

Рассмотрим порядок расчета оптимальных параметров веб-службы. Задача многокритериальной оптимизации включает в себя следующие компоненты:

☑ множество управляемых факторов X (которые представляют собой собственно искомые параметры конфигурирования). Элементами данного множества являются количество фрагментов откликов, средние промежутки времени между ними, а также количество ложных веб-серверов;

Algorithm 1 Алгоритм поиска оптимальных значений параметров веб-службы корпоративных информационных систем

Вход: Общее количество подключений к легитимному веб-серверу L_s, максимальное количество подключений к легитимному веб-серверу L_{smax}, общее количество подключений нарушителя к ложному веб-серверу L_k, максимальное количество подключений нарушителя к ложному веб-серверу L_{kmax}

Выход: количество фрагментов HTTP-ответа (d_i), время между отправкой этих фрагментов (T_i), количество ложных веб-серверов (n_i)

Устанавливают сетевое соединение
$(L_s) \leftarrow$ общее количество подключений всех клиентов к легитимному веб-серверу
if $(L_s > L_{smax})$ then
    (L_s) -= 1
    Выход
if $(L_s \leq L_{smax})$ then
    Принимают команду GET на запрос веб-ресурса
Выделяют идентификатор веб-сессии $(i \in N)$
Принимают команду POST от веб-сервера с предложением авторизации
Задают аутентификационные данные
(N_s) += 1
if $(N_s < 4)$ и аутентификационные данные верны then
    Авторизуют веб-клиента
    Предоставляют легитимному веб-клиенту права доступа к веб-ресурсу
if $(N_s < 4)$ и аутентификационные данные неверны then
    Пытаются авторизоваться снова
if $(N_s \geq 4)$ then
    Выделяют идентификатор веб-сессии нарушителя $(i \notin N, i \in P)$
    (L_s) -= 1
Оценивают значения функции (R), количество фрагментов HTTP-ответа (d_i), время между отправкой этих фрагментов (T_i) и количество ложных веб-серверов (n_i)
(V_s) += 1
$(L_k) = 0$
if $(V_s \geq n_i)$ then
    Завершение веб-сессии
    Выход
if $(V_s < n_i)$ then
    Перенаправляют на ложный веб-сервер
(L_k) += 1
if $(L_k > L_{kmax})$ then
    (V_s) += 1
    Переход к очередному ложному веб-серверу
if $(L_k \leq L_{kmax})$ then
    Задают аутентификационные данные
Формируют и направляют фрагменты HTTP-ответа (d_i) через время (T_i) между отправкой этих фрагментов
if разрыв соединения then
    Завершение веб-сессии
if попытка аутентификации then
    (L_k) += 1
Авторизуют легитимного веб-клиента
Предоставляют веб-клиенту права доступа к веб-ресурсу
Взаимодействуют по принципу запрос-ответ
(L_s) -= 1
Завершают веб-сессию
$(N_s) = 0$
$(V_s) = 0$
Формируют отчет

Рис. 7. Псевдокод алгоритма поиска оптимальных значений параметров веб-службы

- ☑ множество неуправляемых параметров A, характеризующих условия функционирования веб-сессии. Элементами данного множества являются функции распределения длительности ожидания наступления неуправляемых событий;
- ☑ множество целевых функций (или критериев). В качестве целевой функции, характеризующей результативность защиты корпоративных информационных систем, выступает финальная вероятность пребывания системы в состоянии удержания средства сетевой разведки.

В качестве целевой функции, характеризующей доступность ложных веб-серверов, выступает вероятность отказа данной системы, физический смысл которой заключается в невозможности обработки информации ложными веб-серверами.

Задача многокритериальной оптимизации в данном случае формулируется следующим образом: необходимо максимизировать эффективность защиты и минимизировать вероятность отказа системы при соблюдении ряда ограничений и допустимых значений.

$$\begin{cases} F_1(d, T_{res}, n) \longrightarrow \max\limits_{для\ d, T_{res}, n \in N}, \\ F_2(d, T_{res}, n) \longrightarrow \min\limits_{для\ d, T_{res}, n \in N} \end{cases} \quad (14)$$

где целевая функция F_1 характеризует «защищенность» сетевых устройств, а целевая функция F_2 характеризует доступность ложных веб-серверов.

Значения указанных функций и факторов принадлежат области допустимых значений Q:

$$\begin{cases} 0 < n \le 20, \\ 0 < d \le 30, \\ 0 < T_{res} \le 60, \\ \lambda_{12}^V \ge \lambda_{23}^V \ge \lambda_{34}^V \ge \lambda_{35}^V \ge \lambda_{41}^V \ge 0, \\ \lambda_{51}^V \ge \lambda_{61}^V \ge 0 \\ 0 \le F_1(X^V, A^V) \le 1, \\ 0 \le P_{отк} = \left(\frac{\lambda_{nr} \cdot d \cdot T_{res}}{n_{ch}}\right)^n \cdot \frac{1}{\sum_{i=0}^{n} \frac{(\lambda_{nr} \cdot d \cdot T_{res})^i}{i! n_{ch}^i}} \cdot \frac{1}{n!} \le 1 \end{cases} \quad (15)$$

Поскольку задача (14) является многокритериальной, то множество возможных значений целевых функций образует фронт Парето в достижимом критериальном пространстве.

Поиск оптимальных значений был выполнен с использованием метода идеальной точки, суть которого заключается в нахождении точки на фронте Парето, которая максимально близка к идеальной (по заданным критериям).

Таким образом, задача многокритериальной оптимизации (14) сводится к минимизации функции свертки (скалярной функции R), которая получается через частные целевые функции методом отклонения от идеальной точки [14,15] и которая имеет следующий вид:

$$\begin{cases} R(X^V, A^V, X^D, A^D) = \\ = \sqrt{k_1 \cdot \left(\frac{F_1(d, T_{res}, n)}{F_1^{\max}(d, T_{res}, n)} - 1\right)^2 + k_2 \cdot \left(\frac{F_2(d, T_{res}, n)}{F_2^{\max}(d, T_{res}, n)}\right)^2}, \\ R(X^V, A^V, X^D, A^D) \longrightarrow \min\limits_{для\ d, T_{res}, n \in N}. \end{cases} \quad (16)$$

где k_1 и k_2 – коэффициенты значимости, которые отражают предпочтения лица принимающего решения относительно величин частных критериев. Эти коэффициенты могут быть заданы экспертами или получены путем анализа данных.

Поскольку целевые функции (14) имеют различную размерность, то была осуществлена нормировка посредством деления данных целевых функций на их максимальное значение. С условиями данной нормировки, идеальная точка будет иметь координаты (1, 0).

На рисунке 8 представлена визуализация критериального пространства и фронта Парето для различных коэффициентов значимости.

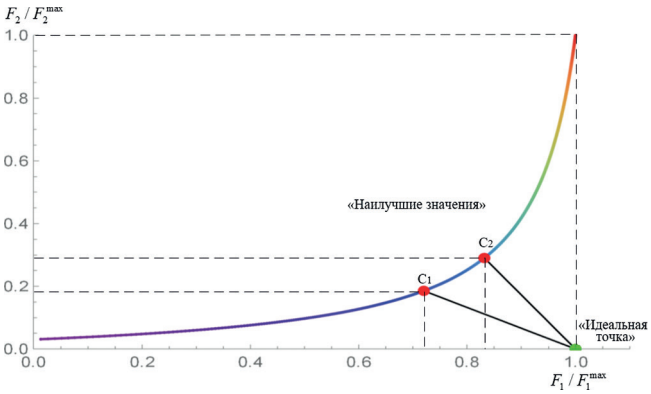

Рис. 8. Критериальное пространство, фронт Парето и два наилучших значения параметров для различных коэффициентов значимости k_1 и k_2

Минимизация скалярной функции R выполнялась с использованием алгоритма «Нелдера-Мида», поскольку благодаря меньшему числу переменных его сходимость была более быстрой (27 миллисекунд) по сравнению с алгоритмом «Имитации отжига» (202 миллисекунды) и алгоритмом «Роя частиц» (1011 миллисекунд).

При обнаружении нарушителя его удержание системой защиты в состоянии ожидания осуществляется на этапе авторизации пользователя, что приводит к снижению результативности проведения сетевой разведки. Результативность разработанного алгоритма была проверена путем его программной реализации и проведения натурного эксперимента в среде программирования Spyder Python и веб-браузере. Суть эксперимента – это оценка длительности взаимодействия веб-сервера и средства сетевой разведки на этапе авторизации при выборе оптимальных режимов конфигурирования параметров

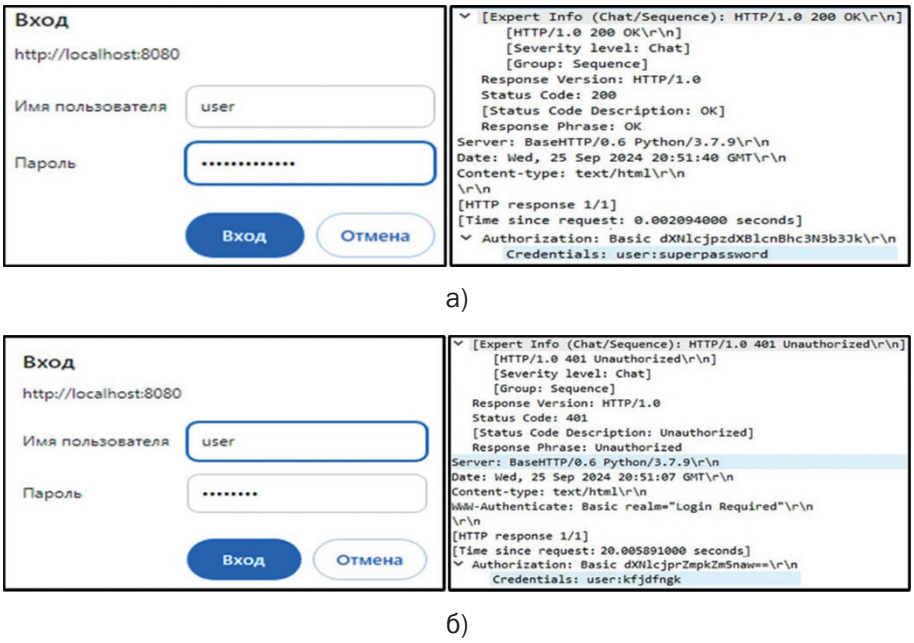

Рис. 9. Авторизация легитимного клиента (а) и попытка авторизации нарушителя (б)

веб-службы. На рисунке 9 продемонстрирована авторизация легитимного клиента (рис. 9а) при условии, что он использует верные аутентификационные данные и попытка авторизации нарушителя (рис. 9б), при условии, что он использует неверные аутентификационные данные. Конфигурирование параметров применяется только при попытке авторизации нарушителя. На рисунке 9б видно, что при конфигурировании параметров веб-службы время HTTP-ответа нарушителю существенно увеличивается.

Проведенный эксперимент показал, что конфигурирование параметров веб-службы корпоративных информационных систем, повышает время удержания средства сетевой разведки в состоянии ожидания, в отличие от ситуации, когда авторизация происходит без конфигурирования параметров. Сравнительный анализ времени авторизации при конфигурировании параметров веб-службы и без него приведен в таблице 6.

Разработанный алгоритм нахождения значений параметров веб-службы для определения оптимальных режимов конфигурирования корпоративных информационных систем позволяет повысить результативности защиты за счет снижения возможностей средств сетевой разведки по подбору имен и паролей санкционированных клиентов, и увеличении временного ресурса, расходуемого средством сетевой разведки, для идентификации средств защиты.

Таблица 6.

Сравнительный анализ времени авторизации при конфигурировании параметров веб-службы и без него

№ п/п	Протокол	Код состояния	Значение пароля	Количество фрагментов HTTP-ответа, шт	Значение времени между фрагментами HTTP-ответа, с	Количество ложных веб-серверов	Время попытки авторизации без конфигурирования параметров веб-службы, с	Время попытки авторизации с конфигурированием параметров веб-службы, с
1.	HTTP	200 OK	superpass-word	–	–	–	0.002094000	–
2.	HTTP	401 UN-AUTHOR-IZED	kfjdfngk	10	2	5	0.002137800	20.005891000
3.	HTTP	401 UN-AUTHOR-IZED	j	7	4	7	0.003309000	28.010590500

Выводы

Разработанная модель позволяет исследовать различные этапы веб-сессии при конфигурировании параметров веб-службы корпоративной сети передачи данных в условиях сетевой разведки. Модель формализована в виде полумарковского случайного процесса с дискретными состояниями и непрерывным временем, при этом выходные характеристики (интервально-переходные вероятности, функции распределения первого достижения соответствующего состояния) определяются через основные характеристики полумарковского процесса с экспоненциальным законом распределения.

Полученные вероятностно-временные характеристики могут быть использованы как целевые функции, которые характеризуют критерии «защищенности» веб-службы и «доступности» ложных веб-серверов в условиях сетевой разведки.

Разработанный алгоритм позволяет определить оптимальный режим конфигурирования параметров веб-службы корпоративных информационных систем. Эффект достигается путем имитации веб-сессии низкого качества на этапе авторизации веб-клиента, за счет варьирования таких параметров, как количество фрагментов HTTP-ответа и время между этими фрагментами. А также за счет добавления ложных веб-серверов, что приводит к увеличению временного ресурса, расходуемого средством сетевой разведки для идентификации средств защиты.

Разработанное научно-методическое обеспечение необходимо для назначения параметров средств защиты веб-серверов при предупреждении и ликвидации компьютерных атак.

Литература

1. *Марков А. С. Важная веха в безопасности открытого программного обеспечения // Вопросы кибербезопасности. 2023. № 1 (53). С. 2–12. DOI:10.21681/2311-3456-2023-1-2-12.*
2. *Соколовский С. П., Горбачев А. А. Способ проактивной защиты почтового сервера от нежелательных сообщений электронной почты // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2021. № 3-4 (153-154). С. 31–40.*
3. *Walla S., Rossow C. MALPITY: Automatic identification and Exploitation of Tarpit Vulnerabilities in Malware. 2019 IEEE European Symposium on Security and Privacy (EuroS&P). 2019. pp. 590–605. DOI: 10.1109//EuroSP.2019.00049.*
4. *Maximov R. V., Sokolovsky S. P., Telenga A. P. Methodology for substantiating the characteristics of false network traffic to simulate information system. CEUR Workshop Proceeding. 2021. pp. 115–124.*
5. *Maximov R. V., Sokolovsky S. P., Telenga A. P. Honeypots network traffic parameters modelling. CEUR Workshop Proceeding. 2021. pp. 229–239.*
6. *Ворончихин И. С., Иванов И. И., Максимов Р. В., Соколовский С. П. Маскирование структуры распределенных информационных систем в киберпространстве // Вопросы кибербезопасности. 2019. № 6(34). С. 92–101. DOI:10.21681/2311-3456-2019-6-92-101.*
7. *Патент № 2716220 Российской Федерации. Способ защиты вычислительных сетей / Р. В. Максимов, С. П. Соколовский, И. С. Ворончихин // заявитель и патентообладатель Краснодарское высшее военное училище имени генерала армии С. М. Штеменко. № 2019123718, заявл. 22.07.2019, опубл. 06.03.2020.*
8. *Патент № 2810193 Российской Федерации. Способ защиты вычислительных сетей / Р. В. Максимов, А. А. Москвин, С. П. Соколовский, В. В. Починок, И. С. Ворончихин, А. П. Теленьга, А. А. Горбачев, С. С. Каверин // заявитель и патентообладатель Краснодарское высшее военное училище имени генерала армии С.М. Штеменко. № 2023100318, заявл. 10.01.2022, опубл. 22.12.2023.*
9. *Евневич Е. Л., Фаткиева Р. Р. Моделирование информационных процессов в условиях конфликтов // Вопросы кибербезопасности. 2020. № 2. С. 42–49. DOI:10.21681/2311-3456-2020-2-42-49.*
10. *Кубарев А. В., Лапсарь А. П., Федорова Я. В. Повышение безопасности эксплуатации значимых объектов критической инфраструктуры с использованием параметрических моделей эволюции // Вопросы кибербезопасности. 2020. № 1 (35). С. 8–17. DOI:10.21681/2311-3456-2020-01-08-17.*
11. *Дроботун Е. Б. Методика снижения удобства использования автоматизированной системы при введении в ее состав системы защиты от компьютерных атак // Вопросы кибербезопасности. 2020. № 2 (36). С. 50–57. DOI:10.21681/2311-3456-2020-02-50-57.*
12. *Будников С. А., Бутрик Е. Е., Соловьев С. В. Моделирование APT-атак, эксплуатирующих уязвимость Zerologon // Вопросы кибербезопасности. 2021. № 6 (46). С. 47–61. DOI:10.21681/2311-3456-2021-6-47-61.*
13. *Горбачев А. А. Модель и параметрическая оптимизация проактивной защиты сервиса электронной почты от сетевой разведки // Вопросы кибербезопасности. 2022. № 3 (49). С. 69–81. DOI:10.21681/4311-3456-2022-3-69-81.*
14. *Шерстобитов Р. С. Модель маскирования информационного обмена в сети передачи данных ведомственного назначения // Системы управления, связи и безопасности. 2024. № 1. С. 1–25. DOI: 10.24412/2410-9916-2024-1-001-025.*
15. *Москвин А. А., Максимов Р. В., Горбачев А. А. Модель, оптимизация и оценка эффективности применения многоадресных сетевых соединений в условиях сетевой разведки // Вопросы кибербезопасности. 2023. № 3 (55). С. 13–22. DOI:10.21681/2311-3456-2023-3-13-22.*

MODEL OF THE OPERATION PROCESS AND ALGORITHM FOR DETERMINING OPTIMAL VALUES OF CONFIGURABLE PARAMETERS OF THE WEB SERVICE OF CORPORATE INFORMATION SYSTEMS

Kaverin S. S.[6], Maksimov R. V.[7], Moskvin A. A.[8]

Keywords: *random process, probabilistic-time characteristics, web resources, ideal point method, web session, interval-transition probabilities.*

The purpose of the study: *increasing the security of the web service of corporate information systems in the context of network reconnaissance.*

Methods used: *Pareto optimization, ideal point, Nelder-Mead, particle swarm, simulated annealing.*

The result of the study: *a model for the functioning of a web service of corporate information systems in network intelligence conditions has been developed, which is implemented in the form of a semi-Markov random process with discrete states and continuous time. The probabilistic-time characteristics of the processes under study were obtained, which are necessary to determine the optimal mode for configuring the parameters of the web service.*

The problem of vector optimization has been solved to determine the optimal values of the parameters of the web service of corporate information systems, such as the number of HTTP response fragments, the time between these fragments, as well as the number of false web servers, allowing to maximize the effectiveness of protecting the web service of corporate information systems and minimize the likelihood failure of false web servers under appropriate restrictions.

Scientific novelty: *consists in developing a model and algorithm for searching the optimal parameters of a web service of corporate information systems in network intelligence conditions using the mathematical apparatus of semi-Markov random processes and scalarization of the vector optimization problem by the ideal point method.*

References

1. *Markov A. S. Vazhnaja veha v bezopasnosti otkrytogo programmnogo obespechenija // Voprosy kiberbezopasnosti. 2023. № 1 (53). S. 2–12. DOI:10.21681/2311-3456-2023-1-2-12.*
2. *Sokolovskij S. P. Model' zashhity informacionnoj sistemy ot setevoj razvedki dinamicheskim upravleniem ee strukturno-funkcional'nymi harakteristikami // Voprosy oboronnoj tehniki. Serija 16 protivodejstvie terrorizmu. 2020. № 7-8. S. 62–73.*
3. *Walla S., Rossow C. MALPITY: Automatic identification and Exploitation of Tarpit Vulnerabilities in Malware. 2019 IEEE European Symposium on Security and Privacy (EuroS&P). 2019. pp. 590–605. DOI: 10.1109/EuroSP.2019.00049.*
4. *Maximov R. V., Sokolovsky S. P., Telenga A. P. Methodology for substantiating the characteristics of false network traffic to simulate information system. CEUR Workshop Proceeding. 2021. pp. 115–124.*
5. *Maximov R. V., Sokolovsky S. P., Telenga A. P. Honeypots network traffic parameters modelling. CEUR Workshop Proceeding. 2021. pp. 229–239.*
6. *Voronchihin I. S., Ivanov I. I., Maximov R. V., Sokolovskij S. P. Maskirovanie struktury raspredelennyh informacionnyh sistem v kiberprostranstve // Voprosy kiberbezopasnosti. 2019. № 6 (34). S. 92–101. DOI:10.21681/2311-3456-2019-6-92-101.*
7. *Patent № 2716220 Rossijskoj Federacii. Sposob zashhity vychislitel'nyh setej / R. V. Maximov, S. P. Sokolovskij, I. S. Voronchihin // zajavitel' i patentoobladatel' Krasnodarskoe vysshee voennoe uchilishhe imeni generala armii S. M. Shtemenko. № 2019123718, zajavl. 22.07.2019, opubl. 06.03.2020.*
8. *Patent № 2810193 Rossijskoj Federacii. Sposob zashhity vychislitel'nyh setej / R. V. Maximov, S. P. Sokolovskij, I. S. Voronchihin // zajavitel' i patentoobladatel' Krasnodarskoe vysshee voennoe uchilishhe imeni generala armii S. M. Shtemenko. № 2023100318, zajavl. 10.01.2022, opubl. 22.12.2023.*
9. *Evnevich E. L., Fatkieva R. R. Modelirovanie informacionnyh processov v uslovijah konfliktov // Voprosy kiberbezopasnosti. 2020. № 2 (36). S. 42–49. DOI:10.21681/2311-3456-2020-2-42-49.*
10. *Kubarev A. V., Lapsar' A. P., Fedorova Ja. V. Povyshenie bezopasnosti jekspluatacii znachimyh ob#ektov kriticheskoj infrastruktury s ispol'zovaniem parametricheskih modelej jevoljucii // Voprosy kiberbezopasnosti. 2020. № 1 (35). S. 8–17. DOI:10.21681/2311-3456-2020-01-08-17.*

6 Sergey S. Kaverin, post graduate student, Krasnodar Higher Military Orders of Zhukov and the October Revolution Red Banner School named after General of the Army S.M. Shtemenko, Krasnodar, Russia. E-mail: sergey_kav995@mail.ru

7 Roman V. Maximov, Dr.Sc., Professor, Honored Inventor of the Russian Federation, Krasnodar Higher Military Orders of Zhukov and the October Revolution Red Banner School named after General of the Army S.M. Shtemenko, Krasnodar, Russia. E-mail: rvmaxim@yandex.ru

8 Artyom A. Moskvin, Ph.D., Krasnodar Higher Military Orders of Zhukov and the October Revolution Red Banner School named after General of the Army S. M. Shtemenko, Krasnodar, Russia. E-mail: tema.kg9012@gmail.com

11. *Drobotun E. B. Metodika snizhenija udobstva ispol'zovanija avtomatizirovannoj sistemy pri vvedenii v ee sostav sistemy zashhity ot komp'juternyh atak // Voprosy kiberbezopasnosti. 2020. № 2 (36). S. 50–57. DOI:10.21681/2311-3456-2020-02-50-57.*
12. *Budnikov S. A., Butrik E. E., Solov'ev S. V. Modelirovanie APT-atak, jekspluatirujushhih ujazvimost' Zerologon // Voprosy kiberbezopasnosti. 2021. № 6 (46). S. 47–61. DOI:10.21681/2311-3456-2021-6-47-61.*
13. *Gorbachev A. A. Model' i parametricheskaja optimizacija proaktivnoj zashhity servisa jelektronnoj pochty ot setevoj razvedki // Voprosy kiberbezopasnosti. 2022. № 3 (49). S. 69–81. DOI:10.21681/4311-3456-2022-3-69-81.*
14. *Sherstobitov R. S. Model' maskirovaniya informacionnogo obmena v seti peredachi dannyh vedomstvennogo naznacheniya // Sistemy upravleniya, svyazi i bezopasnosti. 2024. № 1. S. 1–25. DOI: 10.24412/2410-9916-2024-1-001-025.*
15. *Moskvin A. A., Maximov R. V., Gorbachev A. A. Model', optimizaciya i ocenka effektivnosti primeneniya mnogoadresnyh setevyh soedinenij v usloviyah setevoj razvedki // Voprosy kiberbezopasnosti. 2023. № 3 (55). S. 13–22. DOI:10.21681/2311-3456-2023-3-13-22.*