Теоретические основы информатики

Theoretical foundations of computer science

УДК 002.6, 004.7, 004.722

МЕТОДИКА ОЦЕНКИ УСТОЙЧИВОСТИ ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЕЙ В УСЛОВИЯХ КОМПЬЮТЕРНЫХ АТАК

И. В. КОТЕНКО[1)]***, И. Б. САЕНКО***[1)]***,***
С. Ю. СКОРОБОГАТОВ[1)]***, О. С. ЛАУТА***[2)]***, В. П. КОЧИН***[3)]

[1)]*Санкт-Петербургский федеральный исследовательский центр РАН,*
14-я линия Васильевского острова, 39, 199178, г. Санкт-Петербург, Россия
[2)]*Государственный университет морского и речного флота*
им. адмирала С. О. Макарова, ул. Двинская, 5/7, 198035, г. Санкт-Петербург, Россия
[3)]*Белорусский государственный университет, пр. Независимости, 4, 220030, г. Минск, Беларусь*

Образец цитирования:
Котенко ИВ, Саенко ИБ, Скоробогатов СЮ, Лаута ОС, Кочин ВП. Методика оценки устойчивости программно-конфигурируемых сетей в условиях компьютерных атак. *Журнал Белорусского государственного университета. Математика. Информатика.* 2024;3:90–102.
EDN: WFDUZG

For citation:
Kotenko IV, Saenko IB, Skorobogatov SY, Lauta OS, Kochyn VP. Methodology for assessing the reliability of software-defined networks under computer attacks. *Journal of the Belarusian State University. Mathematics and Informatics.* 2024;3:90–102. Russian.
EDN: WFDUZG

Авторы:
Игорь Витальевич Котенко – заслуженный деятель науки Российской Федерации, доктор технических наук, профессор; главный научный сотрудник.
Игорь Борисович Саенко – доктор технических наук, профессор; ведущий научный сотрудник.
Сергей Юрьевич Скоробогатов – соискатель.
Олег Сергеевич Лаута – доктор технических наук, доцент; профессор кафедры комплексного обеспечения информационной безопасности Института водного транспорта.
Виктор Павлович Кочин – кандидат технических наук, доцент; проректор по учебной работе и интернационализации образования.

Authors:
Igor V. Kotenko, honored scientist of the Russian Federation, doctor of science (engineering), full professor; chief researcher.
ivkote@comsec.spb.ru
Igor B. Saenko, doctor of science (engineering), full professor; leading researcher.
ibsaen@comsec.spb.ru
Sergey Y. Skorobogatov, competitor.
skorobogatovsu-vas@yandex.ru
Oleg S. Lauta, doctor of science (engineering), docent; professor at the department of integrated information security, Water Transport Institute.
laos-82@yandex.ru
Victar P. Kochyn, PhD (engineering), docent; vice-rector for academic affairs and internationalisation of education.
kochyn@bsu.by

Аннотация.

Введение. Важной особенностью технологии программно-конфигурируемых сетей (SDN) является централизованное управление сетью с помощью контроллера, реализованное посредством протокола управления. Контроллер является самым уязвимым элементом SDN, атака на который может повлиять на устойчивость ее функционирования.

Постановка задачи. Разработка математических основ оценки устойчивости SDN позволит с помощью аналитических выражений вычислить показатели устойчивости SDN. В качестве базового показателя предлагается использовать коэффициент исправного действия по устойчивости SDN.

Методы. Оценка показателей устойчивости SDN выполнена с применением методов теории марковских процессов. В целях обеспечения устойчивости функционирования SDN в статье обоснован алгоритм контроля за состоянием контроллеров и их автоматической перестройкой.

Результаты. Осуществлена вербальная и математическая постановка научной задачи на исследование, а общая задача декомпозирована на частные задачи, такие как концептуальное моделирование подсистемы интеллектуального мониторинга состояния информационно-телекоммуникационной сети общего пользования, разработка метода синтеза ее подсистемы интеллектуального мониторинга состояния и формирование научно-технических предложений по реализации данного метода.

Практическая значимость. Предложенная методика позволяет оценить устойчивость SDN в условиях характерных для нее компьютерных атак и, используя полученные показатели устойчивости, сформировать общие требования к системе защиты.

Ключевые слова: компьютерные атаки; устойчивость; программно-конфигурируемые сети; цепи Маркова.

Благодарность. Исследование выполнено за счет гранта Санкт-Петербургского научного фонда № 23-РБ-01-09.

METHODOLOGY FOR ASSESSING THE RELIABILITY OF SOFTWARE-DEFINED NETWORKS UNDER COMPUTER ATTACKS

***I. V. KOTENKO*[a], *I. B. SAENKO*[a], *S. Y. SKOROBOGATOV*[a], *O. S. LAUTA*[b], *V. P. KOCHYN*[c]**

[a]*Saint Petersburg Federal Research Center of the Russian Academy of Sciences, 39, 14th Line V. O., Saint Petersburg 199178, Russia*
[b]*Admiral Makarov State University of Maritime and Inland Shipping, 5/7 Dvinskaja Street, Saint Petersburg 198035, Russia*
[c]*Belarusian State University, 4 Niezaliezhnasci Avenue, Minsk 220030, Belarus*
Corresponding author: V. P. Kochyn (kochyn@bsu.by)

Abstract.

Introduction. An important feature of SDN technology is centralised network management using a controller realised using the OpenFlow control protocol and allowing not only to manage network devices, but also to collect network statistics, which permits to solve emerging network problems more effectively by configuring all network devices simultaneously. The controller is the most vulnerable element, an attack on which can affect the stability of its the entire infrastructure.

Problem statement. The development of mathematical foundations for assessing SDN stability will allow us to calculate SDN stability indicators using analytical expressions. As the main indicator, it is proposed to use the coefficient of serviceable action for SDN stability.

Methods. The estimation of SDN stability indicators is carried out using methods of the theory of Markov processes. In order to ensure the stability of the SDN operation, this paper substantiates an algorithm for monitoring the state of controllers and their automatic adjustment.

Results. A verbal and mathematical formulation of the scientific problem for the study is carried out, and the general problem is decomposed into specific problems, namely, conceptual modelling of the subsystem of intelligent monitoring of the state of the public information and telecommunications network, development of a method for synthesising its subsystem of intelligent monitoring of the state, as well as the formation of scientific and technical proposals for the implementation of this method.

Practical significance. The proposed methodology makes it possible to estimate the stability of a software-defined network in the conditions of computer attacks characteristic for it, as well as to form general requirements for the protection system using the obtained stability indicators.

Keywords: computer attacks; stability; software-defined networks; Markov chains.

Acknowledgements. The research was supported by the Saint Petersburg Science Foundation grant No. 23-RB-01-09.

Введение

Важной особенностью технологии программно-конфигурируемых сетей (software-defined networks, SDN) является централизованное управление сетью с помощью контроллера, реализованное посредством протокола управления OpenFlow, позволяющего не только управлять сетевыми устройствами, но и собирать сетевую статистику, что способствует более эффективному решению возникающих в сети проблем и реконфигурирует одновременно все устройства сети.

Протокол OpenFlow позволяет реализовать управляемую и высоконадежную среду благодаря следующим возможностям [1]:

- модель потока ориентирована на обеспечение безопасности;
- централизованное управление позволяет рационально контролировать производительность сети в условиях кибератак;
- настройка политики безопасности обеспечивается программным контролем;
- сдерживание и изоляция от кибератак осуществляются через гибкое управление трафиком.

Концептуальная структура SDN включает уровень прикладных приложений, API, уровень управления, OpenFlow и уровень передачи данных.

Уровень передачи данных выполняет функции коммутаторов уровней L2 и L3 по обработке и передаче сетевого трафика. Набор правил каждый коммутатор получает от контроллера по каналу управления и протоколу управления OpenFlow. В свою очередь, протокол OpenFlow предоставляет контроллеру возможность использовать специальные таблицы маршрутизации и (или) модификации пакетов. Правила, передаваемые с помощью протокола OpenFlow, могут быть как групповыми, так и дискретными для каждого потока в отдельности. Пакеты, поступившие на входной буфер коммутатора, сначала проверяются на соответствие их заголовков шаблонам правил из нулевой таблицы, а заголовки пакетов сравниваются с шаблонами правил, и в случае совпадения выполняется инструкция согласно выбранному правилу.

В SDN можно выделить три основные составляющие: контроллер, канал управления (OpenFlow) и маршрутизатор (коммутатор) OpenFlow. Как и в классической архитектуре, базовыми элементами являются маршрутизаторы (коммутаторы), которые выполняют обработку сетевого трафика уровней L2 и L3. Однако в данном случае на сетевые устройства возложена функция пересылки трафика между конечными пользователями, а все решения, связанные с фильтрацией и перестроениями маршрутов, которые в классической реализации сети выполняли протоколы динамической маршрутизации, осуществляет контроллер.

Контроллер, в свою очередь, обладает двумя интерфейсами: сервером OpenFlow, который непосредственно управляет сетью и проверяет состояние портов и устройств посредством протокола OF-CONFIG, и интерфейсом API, предоставляемым сетевым приложениям.

Понимание процессов функционирования SDN определяется двумя уровнями технологии SDN: уровнем управления (control plane) и уровнем передачи данных (data plane).

Связь между уровнями осуществляет протокол управления OpenFlow. Для работы протокола управления реализуется соответствующий защищенный канал. Он может быть как отдельным физическим соединением контроллер – коммутатор, так и логическим каналом, проходящим через другие устройства SDN. По каналу управления происходит информационный обмен. Команды управления передаются от контроллера к коммутатору, а информация о состоянии логических переключателей и канала связи между устройствами передается от коммутатора к контроллеру. Одним из основных преимуществ данного решения является централизованное управление. Централизация позволяет динамически изменять маршруты передачи трафика в сети, исходя из меняющейся обстановки. При создании новых маршрутов и подключении новых каналов контроллер, отвечающий за конкретный сегмент, рассылает каждому устройству необходимые правила. Данная особенность существенно отличает SDN от классического подхода, где при изменениях в структуре администратор поэлементно вручную или по протоколам управления SSH/TELNET вынужден прописывать нужные правила [2].

На основе проведенного анализа можно выделить основные векторы угроз для данной концепции. К ним относятся:

- пользователи сети SDN, получающие сетевые услуги;
- канал от пользовательского до сетевого устройства;
- сетевое устройство OpenFlow;
- канал управления и мониторинга OpenFlow;
- контроллер SDN.

Контроллер является ключевым компонентом в управлении всей инфраструктурой SDN, но наиболее уязвимым элементом SDN, поскольку атака на него может повлиять на устойчивость функционирования SDN.

Экономическая парадигма современного мира привела к тому, что разработчики сетевого оборудования экономят на всем, что, в свою очередь, влияет на общую устойчивость информационно-телекоммуникационных сетей, включая SDN. Таким образом, SDN, с одной стороны, создает определенный риск, открывая злоумышленникам новые горизонты, а с другой – дает новые возможности по разработке альтернативных сервисов информационной безопасности [3–5].

Степень разработанности темы

Сегодня известны три основных направления по обеспечению устойчивости SDN в условиях таргетированных (целевых) информационно-технических воздействий [6]. Первый способ – это оптимизация маршрута, используемого для сокращения технологического цикла управления центральным контроллером [7]. В работах [8–10] были рассмотрены вариации усовершенствованного алгоритма Дейкстры по модели взвешенного графа. Для решения задачи маршрутизации потоков в условиях коллизий в работе [11] использован итерационный метод Кларка – Райта, предназначенный для оценки операции слияния между маршрутами. Особенностью этого метода является получение выигрышей путем сокращения стоимости, которое достигается комбинированием двух коротких маршрутов в один большой маршрут. Эвристический метод вставок по принципу «ближайшего соседа», а также его ответвление «табу-поиск» рассматривались в работе [12]. Но, несмотря на простоту решения, данные подходы базируются на формально не обоснованных соображениях.

Второй подход к обеспечению устойчивости SDN – структурный – основан на особенностях архитектуры сети. Часто важным фактором является устойчивость не всей сети, а ее главной части – системы управления. Кибератаки на SDN в 89 % случаев направлены на подсистему управления, так как сбой в ее работе приводит к общему «падению». В исследовании [13] структурная устойчивость SDN оценивается по четырем основным показателям: робастности, возможности резервирования, гибкости управления ресурсом и быстродействию. Такая оценка позволяет отделить процесс маршрутизации от пересылки данных, что является ключевой особенностью для сетей подобного рода.

Ряд исследований в области структурной устойчивости SDN направлены на резервирование контроллеров [14–16] с большим количеством дублируемых трибутарных (tributary) каналов, использование альтернативных алгебраических топологий (например, FatTree) [17], а также на создание гибридов [18–20] разноуровневых топологий, таких как звезда и двойное кольцо, с организацией защиты каналов доступа по принципу 1 + 1. Для всех рассмотренных типов организации структурной устойчивости SDN характерны общие недостатки: несовместимость виртуальной конфигурации с сетевыми контроллерами и высокая стоимость согласованного однотипного «железа» [21].

К третьему варианту повышения устойчивости сети отнесем комбинированные способы, которые сочетают в себе характерные особенности первых двух вариантов. Так, в работе [22] рассмотрен схожий с предлагаемым нами метод превентивного выявления факта воздействия на центральный контроллер SDN, но в отличие от нашего подхода в исследовании [22] систему защиты сети эмулируют на уровне приложений и для отсева аномальных запросов к управляющей подсистеме используют комплементарный фильтр, который, как известно, имеет характерные временные задержки при переходных процессах.

Общим вопросам количественной оценки устойчивости сложных динамических систем, к числу которых относятся SDN, посвящен ряд работ, например [23; 24]. В них исследователи рассматривают устойчивость системы как способность «планировать и готовиться к стихийным бедствиям, поглощать их, реагировать на них и восстанавливаться после них, а также адаптироваться к новым условиям» [24, p. 136]. В этих работах предлагается подход к оценке устойчивости компьютерной сети, основанный на учете критической функциональности и особенностей внешних воздействий на элементы сети. Критическая функциональность может быть определена как качество системы [25], а также как показатель производительности системы, который вводится для получения интегрированного показателя устойчивости (например, критическая функциональность может вычисляться как процент функционирующих узлов).

Таким образом, анализ известных работ по устойчивости компьютерных сетей в условиях воздействия на них компьютерных атак (КА) позволяет сделать следующие выводы:

- стохастическое аналитическое моделирование и методы теории марковских процессов имеют большое значение для обоснования мер защиты в современных системах информационной безопасности;
- с минимальными вычислительными затратами стохастические модели должны рассчитывать функции распределения интересующих нас случайных величин;
- стохастические модели должны обеспечивать моделирование любых атак и высокую гибкость.

Подходы, рассмотренные выше, не в полной мере соответствуют приведенным выводам. В основе описываемого ниже подхода к оценке устойчивости SDN лежат методы теории марковских процессов, так как они позволяют устранить этот недостаток.

Оценивая устойчивость сети, необходимо определить критерии, при которых сеть перестанет выполнять возложенные на нее функции.

При рассмотрении транспортной составляющей разумно предположить, что сеть перестанет быть работоспособной при следующих условиях:

- отказе контроллера транспортной сети либо подмене контроллера в целях управления нарушителем сетью в своих интересах;
- отказе маршрутизаторов, отвечающих за транспортную составляющую сети;
- подмене топологии, при которой нарушитель выдает себя за маршрутизатор транспортной сети и создает черные дыры для передаваемого трафика;
- отказе каналов связи между узлами сети.

Учитывая описанные выше условия, оценим устойчивость SDN при резервировании сетевых устройств. Для этого необходимо представить сеть в виде марковского процесса с дискретными состояниями в непрерывном времени; время пребывания в одном состоянии распределено по показательному закону.

На рис. 1 представлен граф дискретных состояний и условных переходов.

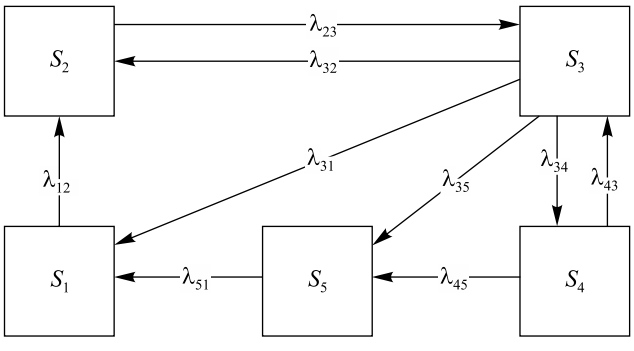

Рис. 1. Граф условных состояний системы передачи данных SDN

Fig. 1. SDN state and transition graph

Заметим, что на графе не рассматривается переход из состояния S_2 в состояние S_5. По нашему мнению, переход из состояния S_2 в состояние S_5 не оказывает большого влияния на устойчивость SDN, так как разведка ведется постоянно и не несет прямой угрозы функционированию сети, требующей восстановления и устранения последствий успешной компьютерной атаки. Иными словами, при составлении мы сделали акцент именно на возможности противодействия КА, но не разведке противника.

В таблице приведено описание условных дискретных состояний распределенной корпоративной SDN в условиях кибератак.

Описание условных дискретных состояний распределенной корпоративной SDN в условиях кибератак

Description of conditional discrete states of distributed enterprise SDN under cyber attacks

Условное обозначение состояния	Описание условного дискретного состояния
S_1	Стабильное устойчивое функционирование без отказов
S_2	Функционирование в условиях технической компьютерной разведки (осуществление нарушителем сбора информации о будущем объекте кибератаки)
S_3	Функционирование в условиях проведения кибератак и в отношении SDN
S_4	Функционирование при успешной атаке (успешное подключение к атакуемой сети, получение доступа к атакуемому контроллеру)
S_5	Обнаружение аномалий в сети, выявление кибератаки, устранение последствий успешной атаки

По нашему мнению, выбор такого количества и состава состояний вполне достаточен для поставленной цели исследования, хотя не исключена возможность дальнейшей детализации состояний. Этот вопрос мы рассматриваем как направление будущих исследований.

Назовем исходные данные для задачи.

1. Граф укрупненных устойчивых состояний SDN в условиях проведения КА $G = (S, \lambda)$.

2. Множество состояний S SDN в условиях ведения КА

$$S = \{S_1, S_2, S_3, S_4, S_5\}.$$

3. Множество потоков событий Λ при изменении состояний SDN в условиях проведения КА

$$\Lambda = \{\lambda_{12}, \lambda_{21}, \lambda_{23}, \ldots, \lambda_{ij}\}.$$

4. Характеристики устойчивых укрупненных состояний SDN при воздействии кибератак. Примером такой характеристики является время прохождения информации. Оно стремится к бесконечности для состояния S_1 и при реализации DDoS-атаки для состояния S_4.

5. Значения интенсивностей потоков событий при воздействии КА, которые получаются следующим образом. Каждая учитываемая КА поэтапно моделируется на имитационной компьютерной модели, построенной в виртуальной среде EVE-NG, в целях получения временных характеристик ее этапов. Далее путем математических расчетов при помощи метода топологического преобразования стохастических сетей [23] получаются искомые значения интенсивностей событий.

6. Вектор вероятностей начальных состояний системы $p_i(0) = \{1, 0, 0, 0, 0, 0, 0\}$.

7. Нормировочное условие

$$\sum_{i=0}^{4} p_i(t) = 1.$$

Моменты вероятностных переходов SDN из одного состояния в другое при использовании стратегии защиты неопределенны, случайны и происходят под действием потоков событий, которые характеризуются интенсивностями $\{\lambda_{ij}\}$. Интенсивности являются важной характеристикой потоков событий и представляют среднее число событий, приходящих за единицу времени. Численные значения интенсивностей зададим в соответствии с имитационной моделью. При решении системы линейных дифференциальных уравнений с постоянными коэффициентами (однородный марковский процесс) переходим к непрерывному времени $t \to 0$. По размеченному графу G сформируем систему дифференциальных уравнений с неизвестными функциями $\{p_i(t)\}$, которые определяют вероятность нахождения системы в состоянии S_i. При этом следуем правилу, что в правой части каждого дифференциального уравнения для $p_i(t)$ произведение $\lambda_{ji}\, p_j(t)$ добавляется со знаком «плюс», а произведение $\lambda_{ij}\, p_i(t)$ – со знаком «минус». Вектор вероятностей начальных состояний системы $\{p_i(0)\}$ необходим для точного решения этой системы.

$$D(P, T) = \begin{cases} \dfrac{dp_1(t)}{dt} = \lambda_{51} p_5(t) + \lambda_{31} p_3(t) - \lambda_{12} p_1(t), \\ \dfrac{dp_2(t)}{dt} = \lambda_{12} p_1(t) + \lambda_{12} p_3(t) - \lambda_{23} p_2(t), \\ \dfrac{dp_3(t)}{dt} = \lambda_{23} p_2(t) + \lambda_{31} p_1(t) + \lambda_{35} p_5(t) + \lambda_{34} p_4(t) - (\lambda_{23} + \lambda_{34}) p_3(t), \\ \dfrac{dp_4(t)}{dt} = \lambda_{43} p_3(t) + \lambda_{45} p_5(t) - \lambda_{34} p_4(t), \\ \dfrac{dp_5(t)}{dt} = \lambda_{51} p_1(t) - (\lambda_{35} + \lambda_{45}) p_5(t), \\ \sum\limits_{i=0}^{4} p_i(t) = 1. \end{cases}$$

Устойчивость SDN является достаточно обширным понятием даже в объеме устойчивости SDN в условиях КА, потому что, как было сказано ранее, появление новых угроз информационной безопасности есть процесс постоянный. Поэтому устойчивость следует рассматривать как способность распределенной корпоративной сети с использованием технологии SDN противостоять определенному классу КА, S_4 является состоянием функционирования SDN при успешном осуществлении КА.

Таким образом, зная вероятность $p_4(t)$ нахождения сети SDN в состоянии S_4, можно найти вероятность устойчивого функционирования всей сети $P_{\text{уст}}(t)$:

$$P_{\text{уст}}(t) = 1 - p_4(t). \quad (1)$$

Блок-схема предлагаемой методики оценки устойчивости распределенной SDN в условиях кибератак имеет вид, представленный на рис. 2.

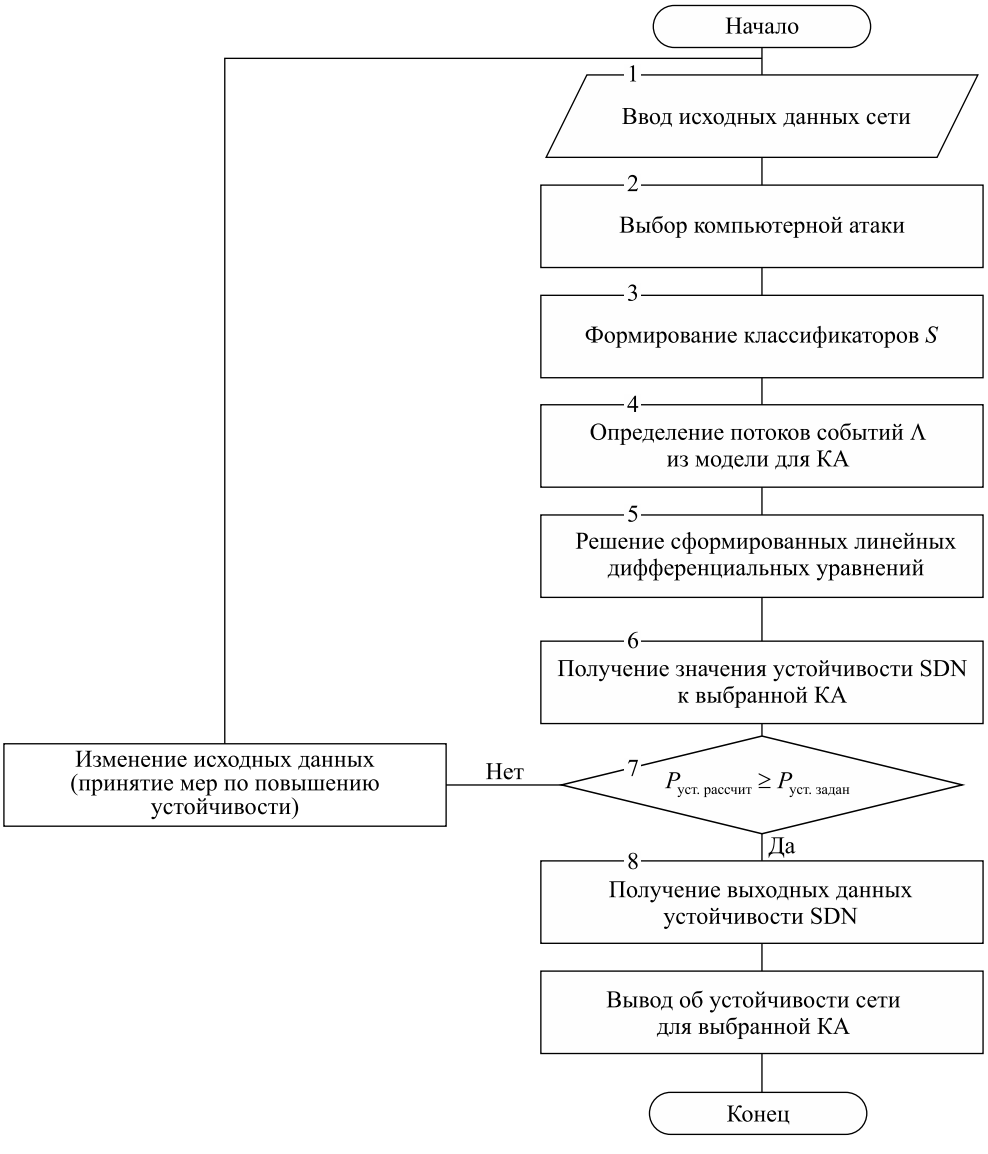

Рис. 2. Блок-схема алгоритма оценки устойчивости SDN в условиях кибератак

Fig. 2. Flowchart of an algorithm describing the technique for assessing the resilience of SDN under cyber attacks

Методика позволяет при определении наиболее актуальных атак для корпоративной SDN рассчитать степень ее устойчивости. Результаты и основанные на них выводы позволяют получить адекватную оценку устойчивости SDN в моделируемых условиях к КА, характерным для данной сети.

Оценка устойчивости SDN в условиях КА

Для оценки устойчивости SDN в условиях КА были разработаны и реализованы три структуры сети:

1) структура SDN, состоящая из трех элементов с одним контроллером;

2) структура SDN на основе двух контроллеров с перехватом функций управления по заданному алгоритму в условиях КА;

3) структура SDN с двумя контроллерами, когда один контроллер является основным и выполняет функции управления, а второй контроллер находится в режиме горячего резервирования.

Результаты расчета представлены в виде графиков (рис. 3–5). Для расчета показателя устойчивости SDN использовалось выражение (1). Пороговое значение 0,2 определяет ориентировочное, на наш взгляд, значение вероятности устойчивого функционирования сети. При значениях показателя устойчивости ниже порогового значения сеть перестает быть устойчивой.

Анализ результатов показал, что рассматриваемые структуры SDN в условиях воздействия КА типов «синхронная атака» и «взлом или сбой контроллера» не соответствуют требованиям по устойчивости. В целях обеспечения устойчивости функционирования SDN в условиях КА необходимо разработать алгоритм контроля за состоянием контроллеров и их автоматической перестройкой, так как через 18 мин успешной реализации КА вероятность устойчивого функционирования сети начинает стремиться к нулю.

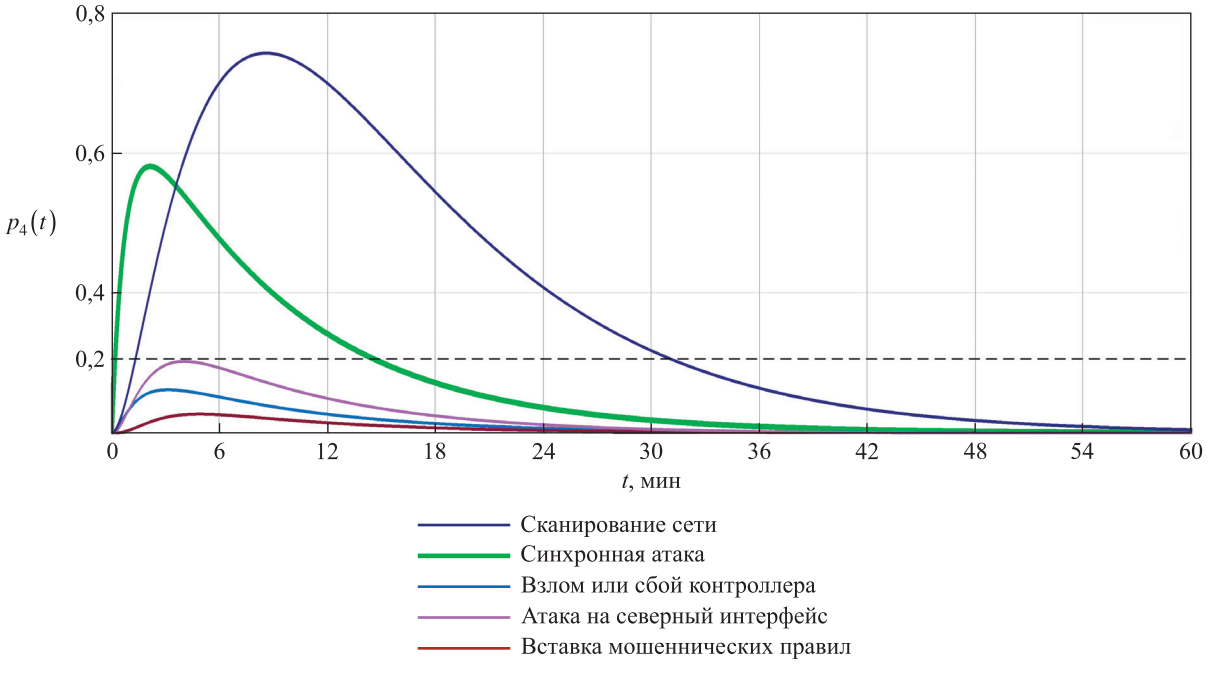

Рис. 3. Зависимость вероятности устойчивой работы SDN от времени реализации КА для структуры 1

Fig. 3. SDN resilience assessment results for structure 1

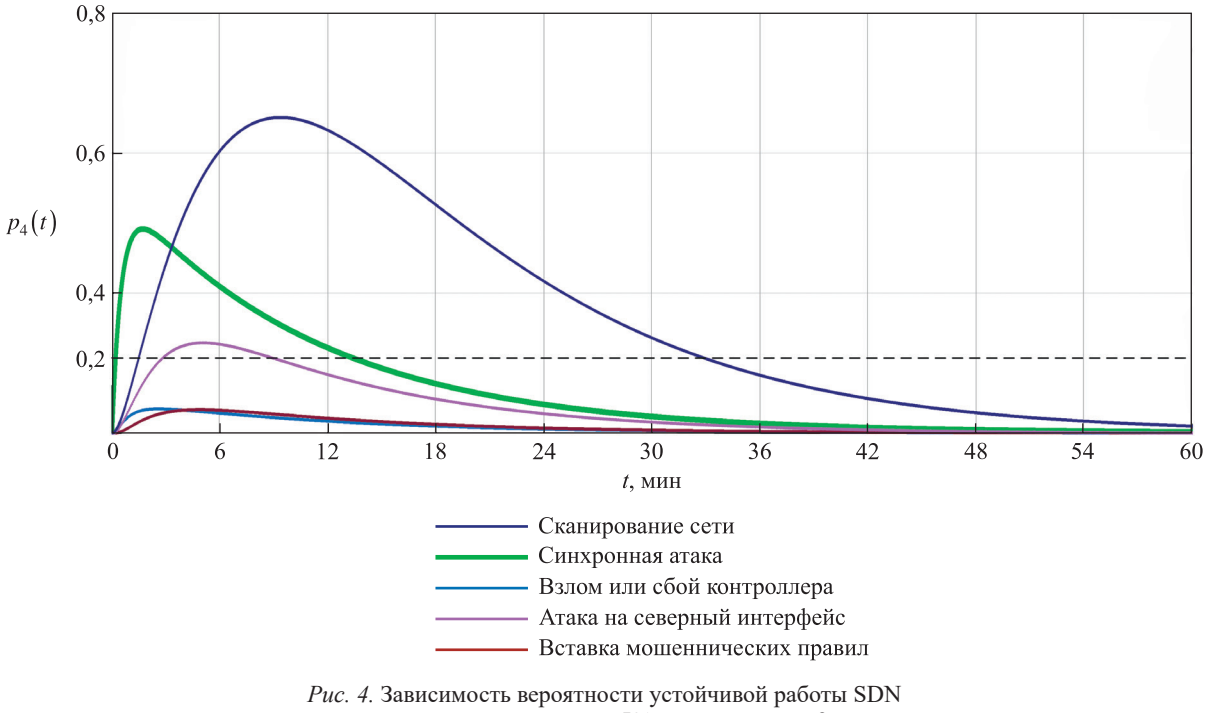

Рис. 4. Зависимость вероятности устойчивой работы SDN от времени реализации КА для структуры 2

Fig. 4. SDN resilience assessment results for structure 2

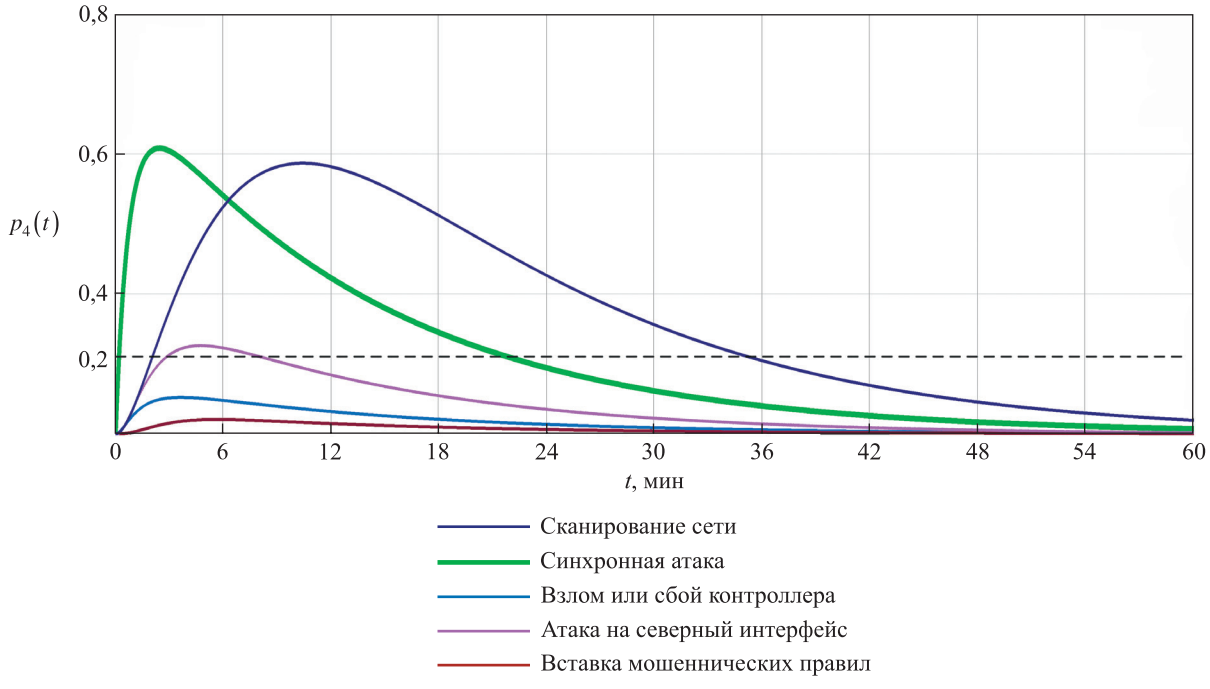

Рис. 5. Зависимость вероятности устойчивой работы SDN от времени реализации КА для структуры 3

Fig. 5. SDN resilience assessment results for structure 3

Таким образом, на базе проведенных исследований по применению SDN, а также по их устойчивости к КА были сформированы общие требования к системе противодействия. Основным способом достижения требуемого уровня устойчивости SDN может стать разработка алгоритмов резервирования контроллеров, а также алгоритмов резервирования и переключения программных коммутаторов.

Алгоритм контроля за состоянием контроллеров и их автоматической перестройкой

Учитывая вышеизложенное, можно сформулировать требования к отказоустойчивому контуру управления SDN, который включает в себя три основных уровня:

1) контур управления уровнем передачи;
2) инфраструктуру мониторинга и управления OpenFlow;
3) межконтроллерную коммуникационную инфраструктуру.

Сложность функционирования такого контура заключается в формировании условий инициирования процессов восстановления SDN при реализации различных КА злоумышленником.

Для решения задачи по повышению устойчивости SDN в условиях КА необходима система защиты (рис. 6), в основу которой заложен алгоритм восстановления сети, выделяющий два уровня:

1) уровень передачи;
2) уровень управления.

При проведении КА злоумышленник осуществляет ряд последовательных действий, при обнаружении которых система защиты должна сигнализировать об этом сетевому администратору, а также рекомендовать применение сценария противодействия. При этом признаки КА для уровней SDN будут различными. Например, для атаки типа «взлом или сбой контроллера», направленной на программный коммутатор, будет характерно повышение трафика, проходящего через контроллер, повышение задержки ответа от контроллера или отсутствие ответа от него, а для атаки типа «взлом или сбой контроллера», направленной на контроллер, – повышение нагрузки процессора, количества запросов и т. д. В этом случае очевидна необходимость разделить условия реагирования программных коммутаторов и контроллеров в зависимости от типов КА.

Для построения системы отказоустойчивости SDN в условиях КА разработана клиент-серверная структура, которая состоит из агентов, функционирующих на программных маршрутизаторах, и сервера, функционирующего на контроллере (рис. 7).

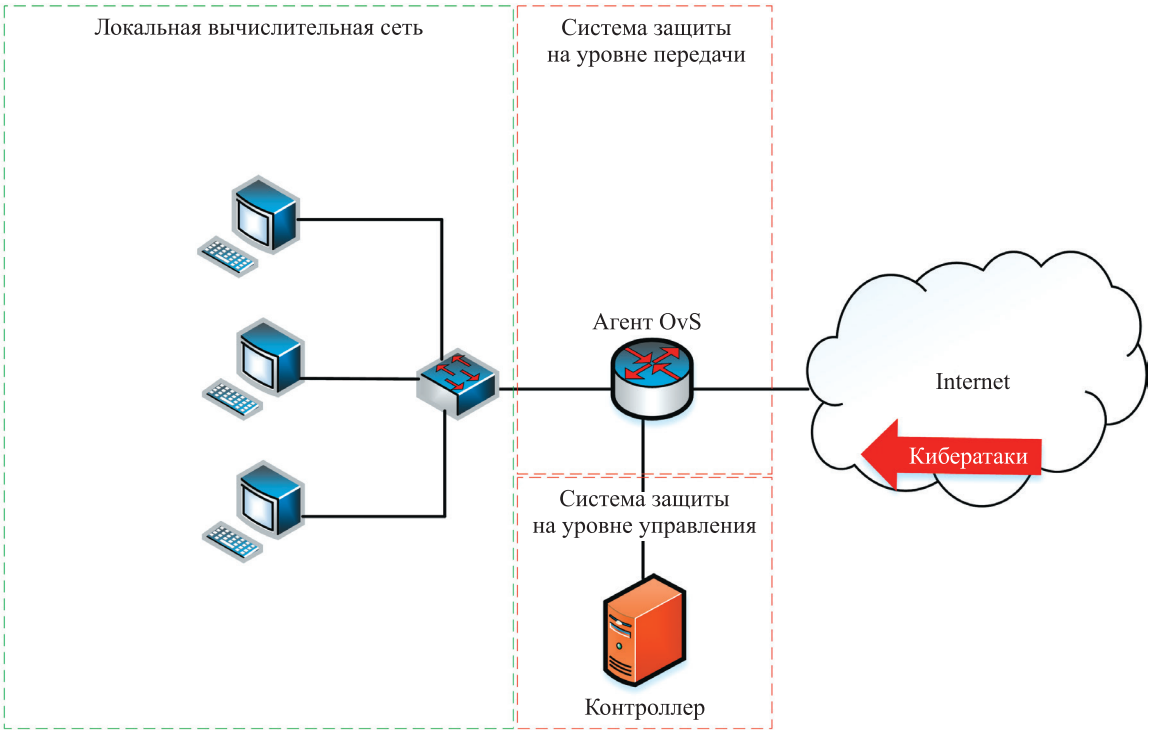

Рис. 6. Вариант предлагаемой структуры построения системы защиты SDN в условиях КА
Fig. 6. A variant of the proposed structure of the SDN protection system in cyberattacks conditions

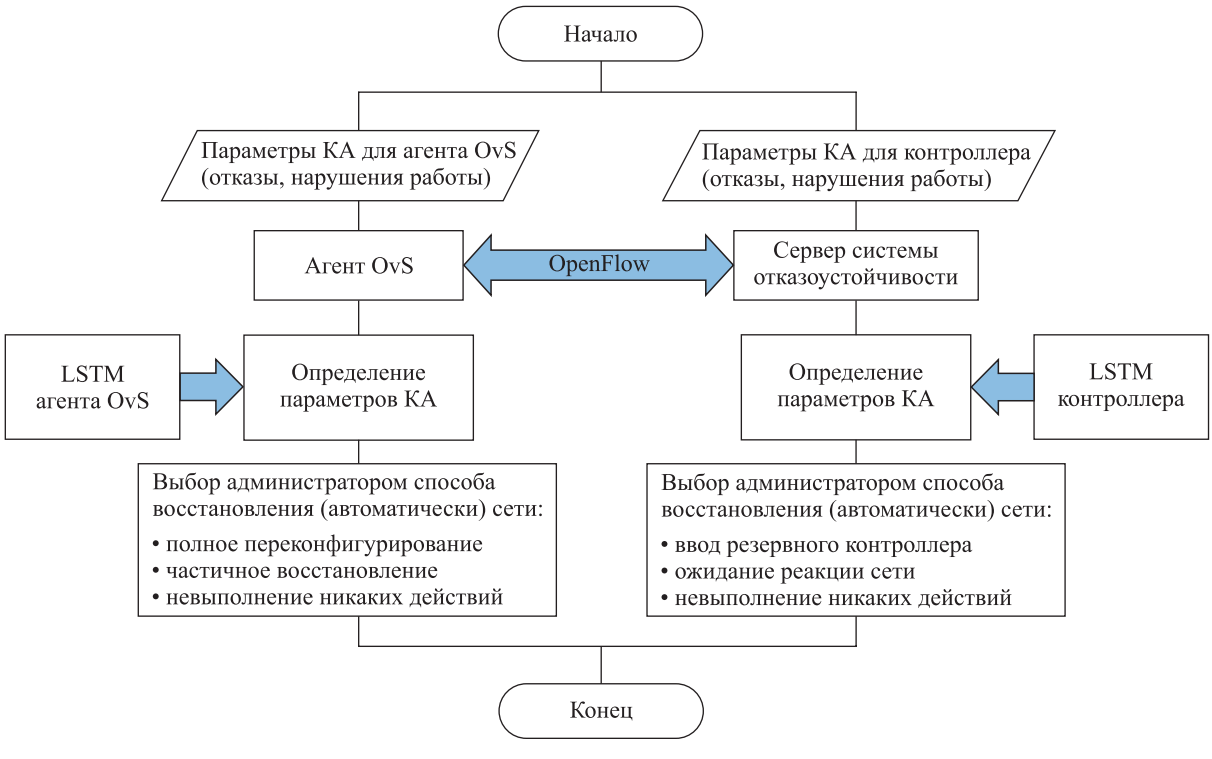

Рис. 7. Обобщенная структура системы обеспечения отказоустойчивости сегмента SDN
Fig. 7. Algorithm for the operation of the fault tolerance system of the SDN segment

Алгоритм восстановления сети в рамках представленной на рис. 6 системы защиты реализуется и увязывается с обобщенной структурой системы обеспечения отказоустойчивости следующим образом. На программном маршрутизаторе (см. рис. 7) работает агент OvS, а на контроллере развернут сервер системы отказоустойчивости, агент OvS и сервер системы отказоустойчивости взаимодействуют по протоколу OpenFlow. Агент OvS является полноценным анализатором аномалий функционирования SDN, в основе которого лежит рекуррентная нейронная сеть с долгой краткосрочной памятью (long short-term memory, LSTM) для программных маршрутизаторов. При этом, определив наиболее вероятный сценарий проводимой атаки, агент OvS предлагает сетевому администратору запуск сценария противодействия (восстановления).

Далее после принятия решения должностным лицом выполняется выбранный сценарий. Из базы данных конфигураций загружается порядок действий, производятся автоматические настройки и подключение к резервному контроллеру при выборе режима полной переконфигурации.

Сервер системы отказоустойчивости запускается в двух версиях – master (ведущий) и slave (подчиненный). Для их совместной работы реализуется сервис синхронизации, который отвечает за переключение контроллеров между собой, а также зеркалирование служебной информации, необходимой для принятия решений на проведение сценария восстановления.

Для определения КА, так же как и в агенте OvS, используется LSTM-сеть. Набор данных, предназначенный для ее обучения, будет отличаться от используемого в агенте OvS. Проводимые КА могут быть направлены на различные элементы сети и вызывать разные последствия. Таким образом, важным фактором функционирования сервера является отсутствие противоречий между выполняемыми агентом сценариями противодействия и сервером системы даже при отсутствии канала управления OpenFlow между ними.

Блок-схема функционирования сервера предлагаемой системы обеспечения устойчивости SDN представлена на рис. 8.

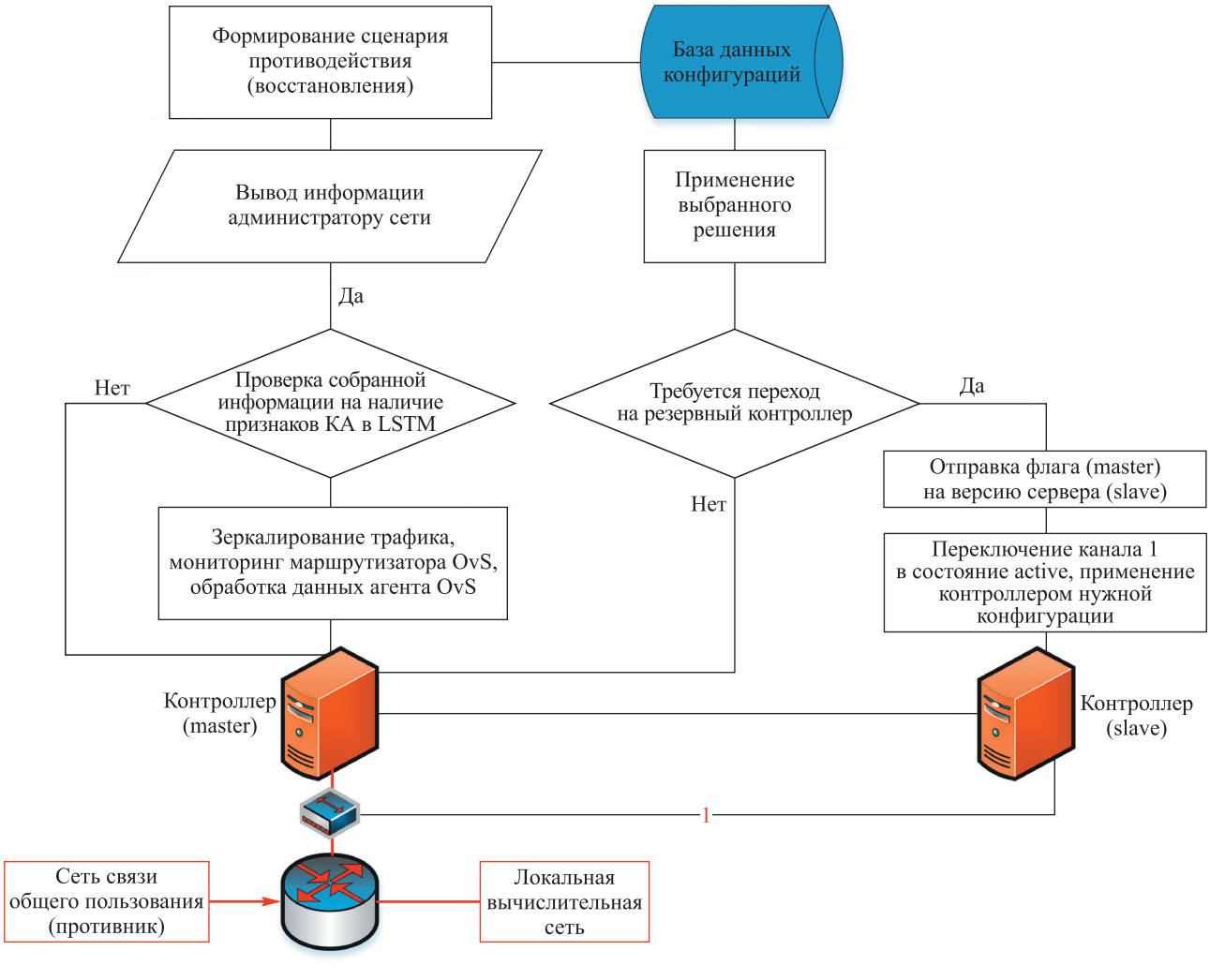

Рис. 8. Блок-схема функционирования сервера системы обеспечения устойчивости SDN

Fig. 8. Functioning diagram for the SDN resilience system server

Таким образом, архитектура системы обеспечения устойчивости SDN состоит из агентов OvS, запускаемых вместе с программными маршрутизаторами и отвечающих за принятие мер по реконфигурации сети в случае обнаружения КА с помощью нейронной сети LSTM, и сервера системы, отвечающего за принятие мер на уровне управления вплоть до ввода в работу резервного контроллера (slave).

Заключение

Проведенный в статье анализ работ, посвященных тематике оценки устойчивости сетей SDN в условиях КА, позволил сделать вывод о том, что стохастическое аналитическое моделирование и методы теории марковских процессов имеют большое значение для обоснования мер защиты в этих сетях, причем стохастические модели должны обеспечивать вычисление функций распределения интересующих нас случайных величин с минимальными вычислительными затратами. На основании результатов проведенного анализа работ по тематике исследования для оценки устойчивости функционирования сетей SDN в условиях КА предложена марковская модель. Одним из состояний графа состояний и переходов марковской модели является функционирование SDN при успешной реализации кибератаки, что позволяет оценить вероятность устойчивости SDN как вероятность противоположного события.

Предложенная марковская модель положена в основу разработанной методики оценки устойчивости сетей SDN в условиях КА, которая позволяет обосновать наиболее устойчивую топологию сети и рассчитать показатели КА. Расчет вероятностно-временных характеристик известных КА осуществляется на базе компьютерного имитационного моделирования в виртуальной среде EVE-NG.

Полученные с помощью предложенной методики вероятностно-временные значения в дальнейшем используются в качестве исходных данных при оценке угроз и обосновании требований по защите SDN от КА. Компьютерное моделирование, проведенное для выбранных в статье вариантов построения сети SDN, продемонстрировало результативность разработанной методики и позволило выработать предложения по архитектуре системы обеспечения устойчивости SDN и ее функционированию. Описанные решения могут быть использованы при проектировании сложных интегрированных систем [26–28].

Дальнейшие исследования будут направлены на разработку аналитических моделей для реализации контрмер в сетях SDN и интеграцию их с моделями кибератак.

Библиографические ссылки

1. Egilmez HE, Dane ST, Bagci KT, Tekalp AM. OpenQoS: an OpenFlow controller design for multimedia delivery with end-to-end quality of service over software-defined networks. In: Asia Pacific Signal and Information Processing Association. *Proceedings of the 2012 Asia Pacific Signal and Information Processing Association annual summit and conference; 2012 December 3–6; Hollywood, USA*. [S. l.]: IEEE; 2012. p. 1–8.

2. Lei Y, Lanson JP, Kaldawy RM, Estrada J, Shue CA. Can host-based SDNs rival the traffic engineering abilities of switch-based SDNs? In: Chemouil P, Krief F, Ahmed T, Hoßfeld T, Secci S, Stanica R, editors. *Proceedings of the 11th International conference on network of the future (NoF); 2020 October 12–14; Bordeaux, France*. [S. l.]: IEEE; 2020. p. 91–99. DOI: 10.1109/NoF50125.2020.9249110.

3. Xia W, Wen Y, Foh CH, Niyato D, Xie H. A survey on software-defined networking. *IEEE Communications Surveys & Tutorials*. 2015;17(1):27–51. DOI: 10.1109/COMST.2014.2330903.

4. Vestin J, Kassler A, Akerberg J. Resilient software defined networking for industrial control networks. In: IEEE. *Proceedings of the 10th International conference on information, communications and signal processing (ICICS); 2015 December 2–4; Singapore*. [S. l.]: IEEE; p. 1–5. DOI: 10.1109/ICICS.2015.7459981.

5. Kreutz DF, Ramos MV, Veríssimo P, Rothenberg CE, Azodolmolky S, Uhlig S. Software-defined networking: a comprehensive survey. *Proceedings of the IEEE*. 2015;103(1):14–76. DOI: 10.1109/JPROC.2014.2371999.

6. Ahmadi V, Jalili A, Khorramizadeh SM, Keshtgari M. A hybrid NSGA-II for solving multiobjective controller placement in SDN. In: Iran University of Science and Technology. *Proceedings of the 2nd International conference on knowledge-based engineering and innovation (KBEI); 2015 November 5–6; Tehran, Iran*. [S. l.]: IEEE; p. 663–669. DOI: 10.1109/KBEI.2015.7436122.

7. Agarwal S, Kodialam M, Lakshman T. Traffic engineering in software defined networks. In: Marsan MA, Colombo G, editors. *Proceedings IEEE INFOCOM; 2013 April 14–19; Turin, Italy*. [S. l.]: IEEE; p. 2211–2219. DOI: 10.1109/INFCOM.2013.6567024.

8. Kotani D, Suzuki K, Shimonishi H. A design and implementation of OpenFlow Controller handling IP multicast with fast tree switching. In: IEEE. *Proceedings of the 12th International symposium on applications and the Internet; 2012 July 16–20; Izmir, Turkey*. [S. l.]: IEEE; p. 60–67. DOI: 10.1109/SAINT.2012.17.

9. Nencioni G, Helvik BE, Gonzalez AJ, Heegaard PE, Kamisinski A. Impact of SDN controllers deployment on network availability. ArXiv:1703.05595 [cs.NI] [Preprint]. 2017 [cited 2024 August 1]: [5 p.]. Available from: https://arxiv.org/abs/1703.05595. DOI: 10.48550/arXiv.1703.05595.

10. Bannour F, Souihi S, Mellouk A. Scalability and reliability aware SDN controller placement strategies. In: IEEE. *Proceedings of the 13th International conference on network and service management (CNSM); 2017 November 26–30; Tokyo, Japan.* [S. l.]: IEEE; 2017; p. 1–4. DOI: 10.23919/CNSM.2017.8255989.

11. Pichpibul T, Kawtummachai R. An improved Clarke and Wright savings algorithm for the capacitated vehicle routing problem. *ScienceAsia*. 2012;38:307–318. DOI: 10.2306/SCIENCEASIA1513-1874.2012.38.307.

12. Ros FJ, Ruiz PM. On reliable controller placements in software-defined networks. *Computer Communications*. 2016;77:41–51. DOI: 10.1016/j.comcom.2015.09.008.

13. Yao G, Bi J, Li Y, Guo L. On the capacitated controller placement problem in software defined networks. *IEEE Communications Letters.* 2014;18(8):1339–1342. DOI: 10.1109/LCOMM.2014.2332341.

14. Park SM, Ju S, Lee J. Efficient routing for traffic offloading in software-defined network. *Procedia Computer Science*. 2014; 34:674–679. DOI: 10.1016/j.procs.2014.07.096.

15. Singh S, Jha RK. A survey on software defined networking: architecture for next generation network. *Journal of Network and Systems Management*. 2017;25(2):321–374. DOI: 10.1007/s10922-016-9393-9.

16. Lange S, Gebert S, Spoerhase J, Rygielski P, Zinner T, Kounev S, et al. Specialized heuristics for the controller placement problem in large scale SDN networks. In: Universiteit Gent. *Proceedings of the 27th International teletraffic congress; 2015 September 8–10; Ghent, Belgium*. [S. l.]: IEEE; 2015. p. 210–218. DOI: 10.1109/ITC.2015.32.

17. Rabia S, I SI, Lilia G, Benjamin K. SDMANET: enhancing MANETs with hybrid protocols through SDN integration. In: IEEE. *Proceedings of the International conference on artificial intelligence, computer, data sciences and applications (ACDSA); 2024 February 1–2; Victoria, Seychelles*. [S. l.]: IEEE; 2024. p. 1–8. DOI: 10.1109/ACDSA59508.2024.10467333.

18. Li J, Chang X, Ren Y, Zhang Z, Wang G. An effective path load balancing mechanism based on SDN. In: IEEE. *Proceedings of the 13th International conference on trust, security and privacy in computing and communications; 2014 September 24–26; Beijing, China.* [S. l.]: IEEE; 2014. p. 527–533. DOI: 10.1109/TrustCom.2014.67.

19. Celenlioglu MR, Alsadi M, Mantar HA. Design, implementation and evaluation of SDN-based resource management model. In: Badra M, Boukerche A, Urien P, editors. *Proceedings of the 7th International conference on new technologies, mobility and security (NTMS); 2015 July 27–29; Paris, France*. [S. l.]: IEEE; 2015. p. 1–8. DOI: 10.1109/NTMS.2015.7266484.

20. Li W, Meng W, Kwok LF. A survey on OpenFlow-based software defined networks: security challenges and countermeasures. *Journal of Network and Computer Applications*. 2016;68:126–139. DOI: 10.1016/j.jnca.2016.04.011.

21. Koushika AM, Selvi ST. Load balancing using software defined networking in cloud environment. In: IEEE. *Proceedings of the International conference on recent trends in information technology; 2014 April 10–12; Chennai, India*. [S. l.]: IEEE; 2019. p. 1–8. DOI: 10.1109/ICRTIT.2014.6996164.

22. Govindarajan K, Meng KC, Ong H, Tat WM, Sivanand S, Leong LS. Realizing the quality of service (QoS) in software-defined networking (SDN) based cloud infrastructure. In: Telkom University. *Proceedings of the 2nd International conference on information and communication technology (ICoICT); 2014 May 28–30; Bandung, Indonesia*. [S. l.]: IEEE; 2014. p. 505–510. DOI: 10.1109/ICoICT. 2014.6914113.

23. Kotenko IV, Saenko IB, Kotsynyak MA, Lauta OS. Assessment of cyber-resilience of computer networks based on simulation of cyber attacks by the stochastic networks conversion method. *SPIIRAS Proceedings*. 2017;6(55):160–184. Russian. DOI: 10.15622/ sp.55.7.

24. Kotenko I, Saenko I, Lauta O. Modeling the impact of cyber attacks. In: Kott A, Linkov I, editors. *Cyber resilience of systems and networks. Risk, systems and decisions*. Cham: Springer; 2019. p. 135–169. DOI: 10.1007/978-3-319-77492-3_7.

25. Lucero B, Viswanathan V, Linsey J, Turner C. Analysis of critical functionality for meta analogy via performance specification. *Proceedings of the International design engineering technical conferences and computers and information in engineering conference*. 2013;2A:DETC2013-13472. DOI: 10.1115/DETC2013-13472.

26. Kochyn V. Conceptual model of complex integrated systems. In: Moscow Polytechnic University. *Proceedings of the 2024 International Russian smart industry conference (SmartIndustryCon); 2024 March 24–30; Sochi, Russia*. [S. l.]: IEEE; 2024. p. 740–745. DOI: 10.1109/SmartIndustryCon61328.2024.10516134.

27. Kochyn VP, Zherelo AV. Designing a secure fail-safe cloud repository of paperworks of students and employees of educational institutions. *Journal of the Belarusian State University. Mathematics and Informatics*. 2021;3:104–108. DOI: 10.33581/2520-6508-2021-3-104-108.

28. Kochyn VP. A model of complex integrated systems. *Journal of the Belarusian State University. Mathematics and Informatics*. 2024;1:71–78. Russian. EDN: NANGXU.

Получена 08.08.2024 / исправлена 23.10.2024 / принята 23.10.2024.
Received 08.08.2024 / revised 23.10.2024 / accepted 23.10.2024.