ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.056
DOI: 10.21822/2073-6185-2023-50-1-62-74 Оригинальная статья /Original Paper

Методика оценки защищённости автоматизированной системы управления критической информационной инфраструктуры от DDoS-атак на основе имитационного моделирования методом Монте-Карло

В.А. Воеводин, В.С. Черняев, Д.С. Буренок, И.В. Виноградов
Национальный исследовательский университет
«Московский институт электронной техники»,
124498, г. Москва, г. Зеленоград, пл. Шокина, 1, Россия

Резюме. Цель. Целью исследования является разработка методики оценки защищённости автоматизированной системы управления критической информационной инфраструктуры (КИИ) от DDoS-атак. Цель разработки методики – предоставить лицу, принимающему решение (ЛПР), научно обоснованный инструмент для оценки риска реализации DDoS-атаки. **Метод.** Для достижения заявленной цели исследования использовалось имитационное моделирование на основе метода Монте-Карло. **Результат.** Подтверждена целесообразность применения имитационного моделирования методом Монте-Карло для оценки вероятности отказа сервера в условиях DDoS-атак. Был сделан вывод о том, что сервер может рассматриваться как система массового обслуживания, однако поток поступающих заявок в условиях DDoS-атак не является пуассоновским, поэтому применение аналитических выражений для оценки вероятности отказа является некорректным. Результаты моделирования позволяют ЛПР оценить вероятность отказа сервера и принять организационные и технические меры для повышения уровня защищённости. Анализ результатов моделирования показал эффективность повышения производительности сервера путём увеличения каналов обслуживания. **Вывод.** Разработанная методика будет полезна при проведении аудита информационной безопасности организации для обоснования размера ее страховой премии в рамках страхования киберрисков. Возможное направление дальнейших исследований – изучение вопроса защищённости вычислительной сети с учётом особенностей конкретной топологии.

Ключевые слова: АСУ ТП, имитационное моделирование, метод Монте-Карло, DDoS-атака, критическая информационная инфраструктура

Для цитирования: В.А. Воеводин, В.С. Черняев, Д.С. Буренок, И.В. Виноградов. Методика оценки защищённости автоматизированной системы управления критической информационной инфраструктуры от DDoS-атак на основе имитационного моделирования методом Монте-Карло. Вестник Дагестанского государственного технического университета. Технические науки. 2023; 50(1):62-74. DOI:10.21822/2073-6185-2023-50-1-62-74

Assessment methodology for security of an automated control system of critical information infrastructure against DDoS attacks based on Monte Carlo simulation

V.A. Voevodin, V.S. Chernyaev, D.S. Burenok, I.V. Vinogradov
National Research University of Electronic Technology,
1 Shokina Square, Moscow, Zelenograd 124498, Russia

Abstract. Objective. The purpose of the study is to develop a methodology for assessing the security of an automated control system of critical information infrastructure from DDoS attacks. The purpose of the methodology development is to provide the decision–maker with a scientifically sound tool for assessing the risk of implementing a DDoS attack. **Method**. To achieve the stated goal of the study, simulation modeling based on the Monte Carlo method was used. **Result**. The expediency of using Monte Carlo simulation to assess the probability of server failure under DDoS attacks is confirmed. It was concluded that the server can be considered as a

queuing system, however, the flow of incoming applications under DDoS attacks is not Poisson, so the use of analytical expressions to assess the probability of failure is considered incorrect. The simulation results allow the decision-maker to assess the probability of server failure and make organizational and technical decisions to increase the level of security. Analysis of the simulation results showed the effectiveness of improving server performance by increasing service channels. **Conclusion.** Thus, the developed methodology will be useful in conducting an information security audit of an organization to justify the amount of its insurance premium in the framework of cyber risk insurance. A possible direction for further research is to study the issue of computer network security, taking into account the features of a specific topology.

Keywords: automated process control system, simulation modeling, Monte Carlo method, DDoS attack, critical information infrastructure

For citation: V.A. Voevodin, V.S. Chernyaev, D.S. Burenok, I.V. Vinogradov. Assessment methodology for security of an automated control system of critical information infrastructure against DDoS attacks based on Monte Carlo simulation. Herald of the Daghestan State Technical University. Technical Science. 2023; 50 (1): 62-74. DOI: 10.21822 /2073-6185-2023-50-1-62-74

Введение. Автоматизированная система управления технологическим процессом (АСУ ТП) – это целостное решение технических и программных средств, которые предназначены для автоматизации управления технологическим оборудованием на промышленных предприятиях [1]. АСУ ТП применяются на объектах КИИ, к которым согласно 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» относятся объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов. Для информационной инфраструктуры АСУ ТП актуален ряд атак, в том числе атаки типа «отказ в обслуживании».

Распределённая атака типа «отказ в обслуживании» или DDoS-атака является одной из наиболее распространённых атак на сетевую инфраструктуру. Механизм данной атаки заключается в создании потока заявок, превышающего максимальный ресурс сервера по обработке запросов, что приводит к отказу в его работе. Источником вредоносных запросов выступают распределённые бот-сети, состоящие из заражённых вирусами компьютеров обычных пользователей, такие компьютеры способны синхронно исполнять команды, передаваемые им с управляющего сервера злоумышленника. Существуют специальные программы и сервисы, с помощью которых возможно организовать DDoS-атаку. Отличительной чертой подобного рода атаки является то, что её реализации практически не оставляет юридически значимых улик. Реализация подобных атак грозит компании существенными финансовыми и репутационными рисками. Для коммерческих организаций финансовый ущерб в среднем достигает порядка нескольких тысяч долларов [2].

Постановка задачи. Вопрос защищённости АСУ от различных угроз, в том числе DDoS-атак, остаётся актуальным и на сегодняшний день. Разработка решений задачи защиты АСУ послужили основой для создания различных практик в этой области, описанных в зарубежных, международных и российских руководящих документах. Актуальность обуславливается необходимостью создания инструмента оценки защищённости АСУ ТП от DDoS-атак для предоставления ЛПР возможности снизить риск возникновения подобной ситуации и особенно обуславливается тем, что вывод из строя АСУ может привести не только к финансовых потерям, но и стать угрозой для жизни и здоровья людей.

Начиная с 2018 года, в России начала формироваться нормативно-правовая база в области безопасности КИИ. Именно тогда вступил в силу федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Данный закон регулирует правовые отношения в области обеспечения безопасности объектов информационной инфраструктуры РФ, имеющих особую значимость для экономики страны. Под действия закона попадают субъекты, работающие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере. Еще к субъектам КИИ относятся предприятия топливно-энергетического комплекса, атомной

энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности.

Правила категорирования КИИ устанавливаются Постановлением Правительства РФ от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

Существуют следующие показатели значимости: социальная, политическая, экономическая, экологическая, а также значимость для обеспечения обороны страны, безопасности государства и правопорядка. Для каждого показателя конкретные значения показателя значимости присваиваются в зависимости от масштаба последствий в случае возникновения инцидентов на объектах КИИ. Нарушение процессов функционирования различных объектов КИИ может иметь различные негативные последствия: от экономического ущерба до причинения вреда жизни и здоровью граждан и угрозам международного уровня. При проектировании системы защиты КИИ учитывается специфика конкретного объекта и, соответственно, применимость к нему других нормативно-правовых актов. Так, если КИИ относится к информационной системе персональных данных, то данный объект попадает под действие [5], и, следовательно, обработка персональных данных должна осуществляться в соответствии с требованиями [6]. Если же объект КИИ относится к государственной информационной системе, определение которой даётся в статье 14 ФЗ-149 «Об информации, информационных технологиях и о защите информации» и которая обрабатывает информацию, не относящуюся к государственной тайне, то требования к защите устанавливаются согласно приказу ФСТЭК России № 17 от 11 февраля 2013 г. «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

АСУ ТП функционируют на объектах КИИ промышленного комплекса. Федеральной службой по техническому и экспортному контролю РФ был разработан ряд требований по защите таких объектов, изложенных в Приказе ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды». Согласно документу обеспечение защиты состоит из пяти этапов:

1) формирование требований;
2) разработка системы защиты;
3) внедрение системы защиты;
4) обеспечение защиты в процессе эксплуатации;
5) обеспечение защиты при выводе из эксплуатации.

Согласно Приказу ФСТЭК России № 31 автоматизированная система управления технологическим процессом имеет многоуровневую структур и состоит их трех уровней:

верхний – уровень операторского управления;
средний – уровень автоматического управления;
нижний – уровень ввода (вывода) данных исполнительных устройств.

К первому уровню относятся операторские, инженерные автоматизированные рабочие места, промышленные серверы (SCADA-серверы), телекоммуникационное оборудование и каналы связи; ко второму уровню относятся программируемые логические контроллеры; к третьему – датчики и исполнительные механизмы.

Следует отметить, что в нормативно-правовой базе, посвящённой информационной безопасности АСУ ТП, важное место занимают документы, регулирующие безопасность отдельных отраслей промышленности. Так, в 2011 году появился №256-ФЗ «О безопасности объектов ТЭК», обязывающий проектировать и внедрять системы обеспечения безопасности объектов ТЭК. Согласно статье 11 данного ФЗ субъекты отрасли должны использовать системы защиты

информации и информационно-телекоммуникационных сетей от неправомерного доступа, уничтожения, модифицирования, блокирования и иных неправомерных действий, а также обеспечивать функционирование таких сетей. Для этого требуется выполнения ряда организационных и технических мероприятий: от определения угроз безопасности до подготовки специалистов в области обеспечения безопасности объектов топливно-энергетического комплекса.

Требования к безопасности тоже должны быть учтены при проектировании. Во время проведения критических операций должен быть обеспечен контроль со стороны человека. Кроме этого, в [7] определён ряд особенностей АСУ ТП, отличающий её от обыкновенной информационной системы:

- АСУ ТП является системой реального времени, следовательно, время реакции критично, особенно в аварийных ситуациях;
- задержки и потери данных неприемлемы;
- для АСУ ТП перезагрузка может быть невозможна вследствие требований к готовности, которые обуславливают необходимость резервирования;
- первостепенную важность имеет безопасность людей, а не возможное нарушение свойств информации (конфиденциальности, целостности, доступности), которая, в свою очередь, зависит от безопасности физических процессов;
- важную роль играет отказоустойчивость – даже кратковременный простой может быть неприемлем;
- наряду с распространёнными операционными системами используются специализированные операционные системы, в том числе без встроенных функций безопасности;
- изменения программного обеспечения (ПО) тщательно контролируются поставщиками ПО вследствие специализированных алгоритмов управления, влияния на конфигурацию аппаратных средств и значительных затрат на лицензирование изменений;
- изменение ПО должны быть протестированы, и должно быть подтверждено сохранение целостности системы после внесения изменений;
- системы разработаны для поддержки промышленных процессов и могут не иметь достаточной памяти или вычислительных ресурсов для поддержки функций безопасности;
- в АСУ ТП применяются специально разработанные коммуникационные протоколы и используются специально проложенные сети;
- продолжительность жизненного цикла может достигать 10-15 лет, для некоторых объектов может доходить до 30 лет.

На основе исходных данных, полученных путём анализа существующих подходов к защите АСУ ТП в России и за рубежом, ставится задача разработки методики оценки защищенности автоматизированной системы управления критической информационной инфраструктуры от DDoS-атак с применением допустимых для решения поставленной задачи методов. Цель применения методики – получение ЛПР информации, достаточной для принятия решения об обработке данного риска и минимизации возможных потерь, либо принятия решения о необходимости принятия риска.

Методы исследования. Применение методов теории систем массового обслуживания (СМО) позволяет решить задачу по оценке вероятности отказа сервера, но при этом требуется принять допущения, которые могут привести к ошибочным результатам. Система массового обслуживания предназначена для обработки заявок и имеет некоторое число обслуживающих единиц – каналов. Согласно [8] различают одноканальные системы с ограничением на длину очереди, одноканальные системы с отказами, многоканальные системы с отказом, многоканальные системы с ограниченной очередью, а также одноканальные и многоканальные системы без ограничений.

Под заявкой понимают объект, поступающий в СМО и требующий обслуживания в обслуживающем приборе. Соответственно, поток заявок – это совокупность заявок, рас-

пределенных во времени. Потоки представляют собой однородные события, которые следуют друг за другом в случайные моменты времени. В случае поступления требований через определённые равные промежутки времени поток называется регулярным. Важнейшими характеристиками являются интенсивность поступления заявок в систему λ и интенсивность обслуживания заявок μ.

Первая величина характеризует частоту появления событий, поступающих в систему массового обслуживания, вторая, соответственно, число заявок, обслуживаемых в единицу времени. Отношение этих двух величин ρ называется коэффициентом загрузки СМО. Для примера, описание процесса в терминах теории СМО можно представить в виде вербальной модели. Пусть на сервер поступают заявки с некоторой интенсивностью λ. При функционировании в штатном режиме закон распределения входного потока этих заявок можно рассматривать как пуассоновский на достаточно большом промежутке времени. Обслуживание поступивших заявок происходит с интенсивностью μ. В качестве обслуживающих каналов выступают процессы-обработчики. Очередь заявок соответствует очереди запросов, приходящих на сервер. В случае занятости всех каналов и мест в очереди происходит отказ, что соответствует переполнению очереди запросов на реальном сервере, что приводит к ошибке «502 Bad Gateway».

Таким образом, разработанная модель соответствует многоканальной системе с ограниченной очередью и ограниченным временем ожидания в очереди. Дисциплина ожидания FIFO (First In, First Out): чем раньше заявка попала в очередь, тем раньше она будет обслужена, приоритет заявок отсутствует.

На рис. 1 представлен размеченный граф состояний системы, в котором состояние S_0 соответствует ситуации, когда все каналы свободны и очередь отсутствует, состояние S_l соответствует ситуации, когда занято l каналов, очереди нет, состояние S_{n+i} показывает, что обслуживанием заявок заняты все n каналов в очереди находятся i каналов, состояние S_{n+m} соответствует случаю, когда все n каналов и m мест в очереди заняты. Величина ν характеризует интенсивность ухода заявок из очереди, что соответствует уходу заявок из очереди сервера вследствие превышения максимального времени нахождения в ней и наступлению ошибки 504 Gateway Time-out.

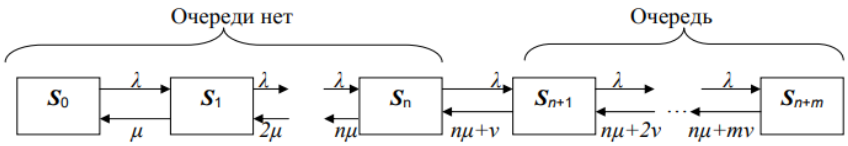

Рис.1. Обобщённый граф состояний многоканальной системы с ограниченной очередью и ограниченным временем ожидания в очереди
Fig.1. Generalized graph of states of a multichannel system with a limited queue and a limited waiting time in the queue

Существуют аналитические методы расчёта вероятности пребывания системы в каждом из l состояний. Например, для рассматриваемой многоканальной системы с ограниченной очередью и временем ожидания в очереди справедливы следующие соотношения для расчёта среднего числа заявок, находящихся в очереди (1), и среднего числа заявок, обслуживаемых в СМО (2) [9]. Однако формулы, приведенные в [9], для решения поставленной задачи не пригодны, так как при моделировании DDoS-атаки на сервер в отдельный момент времени τ на сервер может прийти несколько заявок, что нарушает требования ординарности для потока входящих заявок, и, следовательно, его уже нельзя считать пуассоновским без грубых допущений, которые могут привести к недопустимым ошибочным результатам.

Потребность в исследовании сложных систем послужила толчком для развития теоретических методов познания, важное место среди которых занимает моделирование. Сущность моделирования заключается в воспроизведении отдельных свойств реальных объектов, предметов и явлений с помощью других объектов, процессов, явлений, либо с помощью абстракт-

ного описания. Моделирование всегда опирается на объект исследования, так как информация об объекте и является основой для создания модели. Моделирование особенно актуально на сегодняшний день, так как потребность в исследовании сложных систем заметно возросла. Для сложных систем характерен ряд признаков [10]:

1. Целостность и возможность разделения на части – данное свойство отражает возможность разделения системы на подсистемы, но и свидетельствует о том, что система способна функционировать как единая структура;
2. Наличие связей – это свойство выражается в наличии некоторых каналов передачи информации между элементами, системами, элементами системы и внешним миром;
3. Наличие организации – данное свойство означает, что связи элементов некоторым образом упорядочены и образуют структуру системы;
4. Наличие интегративных качеств – данное свойство тоже означает, что, хотя система зависит от составных элементов, она имеет качества, присущие ей в целом. Данный факт позволяет сделать важный вывод о том, что изучение сложной системы не может быть сведено только к изучению отдельных её частей, и, наоборот, система в целом исследуется, исходя из свойств отдельных её составляющих;
5. Уникальность – сложные системы, как правило, отличаются уникальностью, что требует создания отдельной модели для изучения каждой такой системы;
6. Случайность и неопределённость действующих факторов;
7. Учёт многочисленных факторов, влияющих на систему, увеличивает объём вычислений и существенно усложняет модель, однако вместе с этим повышает её точность;
8. Многокритериальность оценок процессов, протекающих в системе;
9. Невозможность однозначной оценки обуславливается наличием множества подсистем и различных показателей.

Согласно [11] различают следующие виды моделирования: детерминированное, стохастическое, динамическое, дискретное, непрерывное, дискретно-непрерывное, мысленное, наглядное, гипотетическое, аналоговое, макетирование, языковое, аналитическое, математическое моделирование, а также имитационное моделирование.

Следует отметить, что в последнее время наблюдается комбинирование различных видов моделирования. Так, например, имитационное моделирование сочетает в себе признаки концептуального моделирования на ранних этапах формирования моделей и логико-математическое для описания отдельных подсистем и процессов модели, а также при обработке и анализе результатов вычислительного эксперимента. Также, имитационное моделирование наряду со структурно-функциональным моделированием относится к методам компьютерного моделирования.

Метод имитационного моделирования является экспериментальным методом исследования реальной системы по ее компьютерной модели, сочетая особенности экспериментального подхода и использование средств вычислительной техники. То есть, имитационная модель состоит из совокупности реальной системы, логико-математической модели, имитационной модели и электронно-вычислительной машины. Отличительной особенностью имитационного моделирования является сохранение логической структуры моделируемых объектов и динамики взаимодействия элементов, достигаемое посредством описания состояний системы с помощью наборов переменных состояний, изменение которых характеризует переход из состояния в состояние. Таким образом, имитационное моделирование позволяет отразить изменение состояния системы во времени.

Для описания динамического изменения процессов в имитационном моделировании используется модельное время. Модельное время выступает некоторым временным эталоном в системе, что позволяет синхронизировать все протекающие в системе процессы. Различают пошаговое и пособытийное изменение модельного времени.

В первом случае изменение времени происходит постоянно с одинаковой минимально возможной длиной шага, во втором случае изменение времени происходит только при изменении состояния системы. Второй способ более эффективен с точки зрения использования ма-

шинного времени, поэтому является более распространённым. На основе этих двух подходов к организации машинного времени строится классификация имитационных моделей. Выделяют непрерывные, дискретные и непрерывно-дискретные имитационные модели. В первом виде моделей изменение состояния моделируемой системы происходит непрерывно и часто описывается системой дифференциальных уравнений, поэтому продвижение модельного времени будет зависеть от численного решения этих уравнений.

Общая последовательность действий при проведении имитационного моделирования следующая: после изучения реальной системы происходит построение логико-математической модели, затем следует разработка моделирующего алгоритма, построение имитационной модели, планирование и проведение имитационных экспериментов, обработка и анализ результатов и, наконец, принятие решений. Имитационное моделирование является универсальным средством для исследования сложных систем и представляет собой логико-алгоритмическое описание поведения отдельных элементов системы и правил их взаимодействия, отображающих последовательность событий, возникающих в моделируемой системе. Согласно [12] имитационные модели подразделяются на статические (в случае, когда система остаётся неизменной в течение времени), динамические, детерминированные (в случае, когда система не содержит случайных величин) стохастические, непрерывные и дискретные. Используемый в настоящем исследовании метод Монте-Карло относится к методам статического, непрерывного, стохастического моделирования.

Представленное выше описание сервера в терминах теории СМО подходит, например, для серверов с Nginx. Количество каналов, длина очереди, максимальное время пребывания в очереди задаются в конфигурационных файлах Nginx параметрами «worker_connections», «backlog», «timeout», соответственно. Схема обработки запросов Nginx представлена на рис. 2. Множество других сетевых приложений, например, Apache, устроены аналогично.

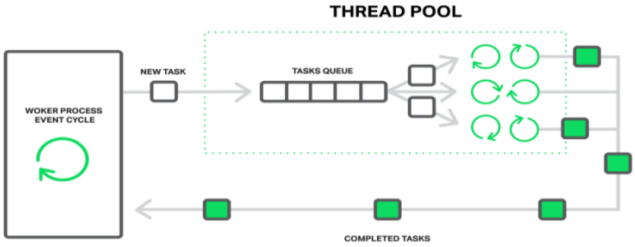

Рис.2. Nginx структура рабочего процесса
Fig.2. Nginx worker process structure

В случае если DDoS-атака ведется на уровне приложения, важно учитывать обращение сервера к базе данных. Она может располагаться как внутри компьютерной сети, так и с привлечением облачным сервисов, центров обработки данных. На транспортном и сетевом уровне обращений к базе данных не происходит, взаимодействие с ней можно не моделировать. Существуют аналитические выражения, с помощью которых можно рассчитать вероятность нахождения СМО в каждом из состояний, а также вероятность отказа. Однако в условиях DDoS-атак их применение является некорректным, так как при моделировании DDoS-атаки на сервер в отдельный момент времени на сервер может прийти несколько заявок, что нарушает требования ординарности для потока входящих заявок, и, следовательно, его уже нельзя считать пуассоновским без грубых допущений, которые могут привести к недопустимым ошибочным результатам [13]. Таким образом, классический инструментарий теории СМО является неприспособленным для решения поставленной задачи. Выходом является применение имитационного моделирования методом Монте-Карло. Имитационное моделирование позволяет отслеживать изменения состояний системы во времени и хорошо применимо для моделирования случайных процессов, таких как DDoS-атаки [14, 15]. В общем случае, разработка имитационной модели дискретных систем, имеющих стохастический характер функционирования, к которым относятся СМО, производится в следующем порядке:

1. Задание закона распределения случайной величины;
2. Генерация значений случайных величин с заданным законом распределения;
3. Формирование потоков заявок и имитация обслуживания;
4. Моделирование очередей заявок на обслуживание;
5. Обработка результатов моделирования.

В качестве средства для проведения в настоящем исследовании использовался пакет электронных таблиц «Microsoft Excel». На сегодняшний день имитация с помощью табличных процессоров выросло в отдельное направление моделирования, имеющее свои особенности. Сторонники подобного моделирования отмечают, что использование данных систем позволяет получить лучшее понимание происходящих процессов по сравнению с применением специализированного ПО. Подобное ПО имеет высокую стоимость и требует существенных временных затрат для его изучения, а также не позволяет понять используемые механизмы, работая, фактически, по принципу «чёрного ящика». Однако, вместе с этим, такие среды предоставляют больше возможностей и позволяют моделировать сложные системы. При реализации моделей в «Microsoft Excel» используют три основных подхода к проведению имитации: ориентированный на события, ориентированный на процессы, сканирования активностей (рис. 3).

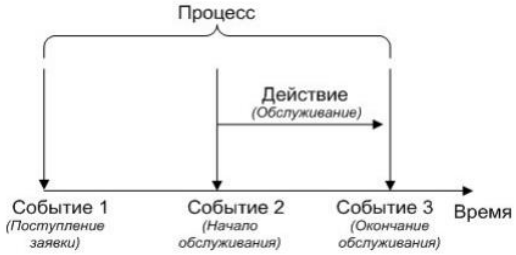

Рис.3. Связь событий, действий и процесса
Fig.3. Connection of events, actions and process

Первый подход описывает изменения в системе, происходящие в момент совершения каждого случайного события (прибытие заявки, завершение обслуживания), и, при его реализации с помощью электронных таблиц, как правило, используется одна строка для каждого события. При использовании процессно-ориентированного подхода происходит моделирование последовательности событий для каждой заявки, и для его реализации обычно используется одна строка для каждого требования (применяется при моделировании СМО). Подход сканирования активностей описывает действия, возникающие в системе в течение фиксированного интервала времени (например, в день, неделю, месяц, год), и при его реализации обычно используется одна строка для каждого временного интервала.

Рассмотрим основные преимущества использования пакета «Microsoft Excel» [16]:

1. Данный пакет насчитывает большое количество различных функций – математических, статистических, финансовых, и других видов встроенных функций. Также имеются специальные функции для генерирования случайных величин;
2. Электронные таблицы позволяют хранить данные в удобном виде и осуществлять доступ к ним;
3. Имеется возможность построения графиков и диаграмм;
4. Программный пакет содержит встроенный язык Visual Basic for Applications;
5. Данное ПО является широко распространенным, так как входит в базовый набор программ пакета «Microsoft Office»;
6. Возможен экспорт в другие программные продукты;
7. Используемые математические функции проверены и верифицированы;
8. В электронных таблицах имеется возможность просмотра всех формул, занесенных в ячейки таблицы, что повышает доверие к результатам моделирования, а с реализованной моделью пользователь может экспериментировать и оценивать результа-

ты без привлечения специалистов в области имитационного моделирования, что также повышает доверие к получаемым результатам;

9. Программный пакет имеет достаточную производительность для решения поставленной задачи.

Обсуждение результатов. Имитационная модель функционирует по следующему алгоритму:

1. Временной шаг задаётся в столбце «Время» и выбран равным 0,1 секунды.

2. В отдельном блоке таблицы задаются интенсивность поступления заявок λ и интенсивность обслуживания μ. Длина очереди и количество каналов являются константами.

λ	10
μ	2
dt	0,1
Максимальное ожидание (в тактах)	6
Длина очереди	3
Количество каналов	3

Рис.4. Блок задания исходных данных
Fig.4. Source data assignment block

3. Приход заявки симулируется функцией генерацией случайного числа от 0 до 1 функцией СЛЧИС() в столбце «RND заявка». Процесс поступления заявки задаётся следующим условием: если случайная величина «RND заявка» меньше произведения λ на dt, то считаем, что заявка поступила. Результат отображается в столбце «Заявка».

4. Столбцы «RND обслужил канал 1», «RND обслужил канал 2», «RND обслужил канал 3» задают случайные величины, характеризующие обслуживание первого, второго и третьего канала соответственно. Событие обслуживание канала симулируется аналогично: если случайная величина «RND обслужил канал 1» меньше произведения μ на dt, то считается, что канал был обслужен. Результат отображается в столбцах «Процесс обслужил канал 1», «Процесс обслужил канал 2», «Процесс обслужил канал 3».

5. Столбцы «Занят канал 1», «Занят канал 2», «Занят канал 3» содержат логический флаг, указывающий на занятость канала или его свободное состояние.

Состояние освобождения каналов (столбцы «Освободился канал 1», «Освободился канал 2», «Освободился канал 3») описывается логическим условием, когда каналы были заняты и их обслужили. Канал 1 получает заявку, если он был свободен или освободился и поступила заявка. Канал 2 получает заявку из очереди, если он свободен и в очереди есть заявки и предыдущий канал (Канал 1) занят. Канал 3 получает заявку из очереди, если он свободен и в очереди есть заявки и предыдущий канал (Канал 2) занят. В имитационной модели отражается событие удаления заявок из очереди при превышении максимального времени ожидания, а также фиксируется время ожидания на каждом из мест в очереди (рис. 5).

заявка была удалена из очереди	занято мест в очереди	время очереди место 1	время очереди место 2	время очереди место 3
0	0	0	0	0
0	0	0	0	0
0	0	0	0	0
0	0	0	0	0
0	1	4	0	0
0	1	5	0	0
0	2	5	6	0
0	0	0	0	0

Рис.5. Столбцы, отвечающие за удаление заявок из очереди и фиксацию времени нахождения в очереди
Fig.5. Columns responsible for removing applications from the queue and fixing the time spent in the queue

Количество отказов рассчитывается как отношение отказов к общему числу заявок (рис. 6).

λ	10
μ	2
dt	0,1
Макс ожидание (в тактах)	6
Длина очереди	3
Количество каналов	3
Отказы (Отношение отказов ко всем заявкам)	0,3876

Рис.6. Расчёт количества отказов
Fig.6. Calculating the number of failures

В имитационной модели предусмотрен автоматический вывод результатов последних 100 симуляций по нажатию кнопки «Вывод» (рис. 7).

	Кнопка для вывода отказов 100 последних симуляций:	Вывод
10		
11	0,07866075	
12	0,060727127	
13	0,075350701	
14	0,070341423	
15	0,074568289	
16	0,043621399	
17	0,069233761	
18	0,072264836	
19	0,073051948	
20	0,085005903	

Лист1

Рис.7. Блок вывода результатов последних 100 симуляций
Fig.7. The block for displaying the results of the last 100 simulations

В основе имитационной модели лежит случайный характер прихода заявок в каждый момент времени. Дальнейшее обслуживание заявок и освобождение каналов описывается с помощью логических выражений.

Процент успешных DDoS-атак, равный вероятности отказа сервера, рассчитывается как отношение отказов к общему числу заявок. В качестве параметров первоначальной модели выступают интенсивность поступления заявок λ и интенсивность обслуживания μ, максимальное ожидание заявки в очереди, длина очереди, количество каналов, а также временной шаг *dt*, который задаётся равным 0,1 секунды. Модель была протестирована при различных величинах отношения λ к μ, что имеет смысл ρ – коэффициента загрузки сервера. Анализ показал, что уже при ситуации, когда интенсивность поступления заявок превышает интенсивность обслуживания в 6,25 раза, вероятность успешной DDoS-атаки оценивается в 51,32%, а при превышении интенсивность поступления заявок в 10 раз вероятность отказа сервера возрастает до 70% (рис. 8).

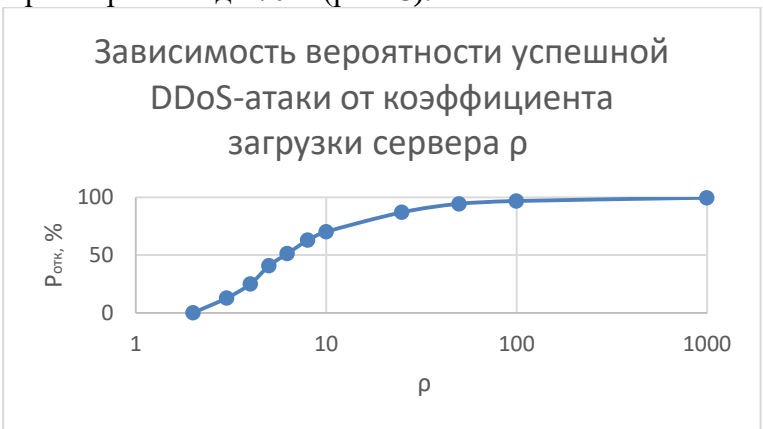

Рис.8. Зависимость вероятности успешной DDoS-атаки от загрузки сервера
Fig.8. Dependence of the probability of a successful DDoS attack on the server load

Для оценки вероятности отказа сервера при большом количестве итераций и произвольном количестве каналов используется программа оценки защищённости сервера от DDoS-атак, принимающая на вход статистику поступления заявок на сервер, длину очереди и максимальное ожидание заявки в очереди [17]. Статистика поступления заявок загружается в виде Excel-файла, в котором первый столбец соответствует поступлению заявок на сервер, последующие столбцы – обслуживанию заявки первым и последующими каналами. Наступление событий поступления заявки и её обслуживания каналом обозначается единицей в соответствующей ячейке, противоположное событие – нулем.

На выходе программа выдаёт вероятность отказа, которая рассчитывается как отношение количество отказов к общему количеству заявок.

Отличительной особенностью программной модели является её универсальность, обуславливающаяся гибкостью изменения параметров. Вычислительных ресурсов программы хватает для 10^6 итераций, после чего данные можно выгрузить на диск. На рис. 9 представлен интерфейс программы.

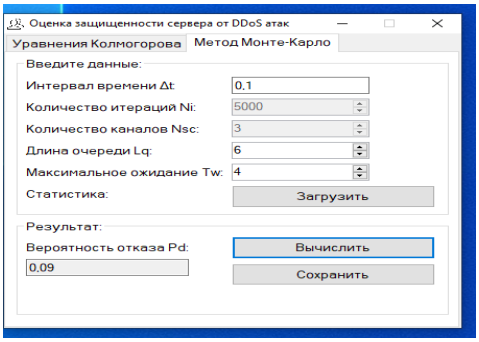

Рис.9. Интерфейс программы
Fig.9. Program interface

Эксперименты, проведённые с моделью, показали, что в условиях высокой интенсивности поступления заявок и высоком значении отношения λ к μ (ρ = 1000), что соответствует DDoS-атаке, вероятность отказа снижается на 4-6% при увеличении количества каналов на пять единиц (рис. 10).

Увеличение очереди обслуживания на 100 единиц позволяет снизить вероятность отказа на 1%.

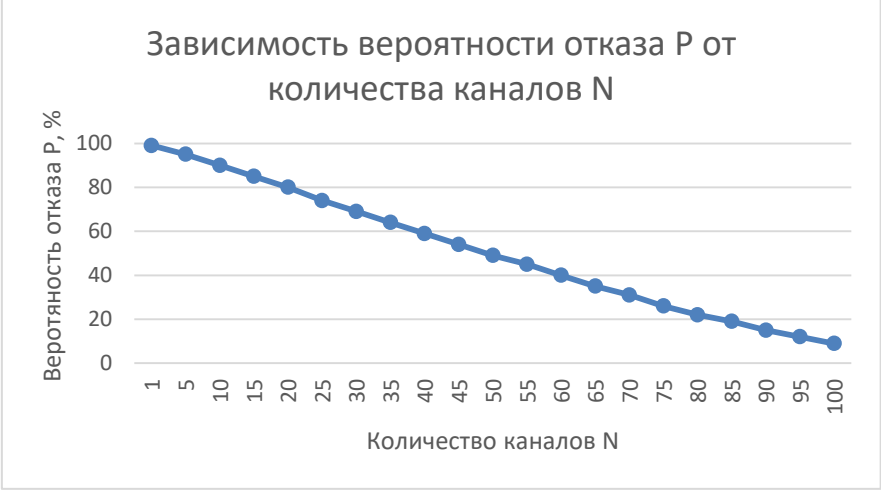

Рис.10. Зависимость вероятности отказа от количества каналов
Fig.10. Dependence of the probability of failure on the number of channels

Так, при начальной вероятности отказа, равной 80%, и длине очереди, равной единице, для снижения вероятности отказа до 50% потребовалось увеличение очереди до 3000 единиц (рис. 11). Полученные результаты свидетельствуют о том, что наиболее эффективным способом снижения вероятности отказа является повышение производительности сервера путём увеличения его каналов обслуживания.

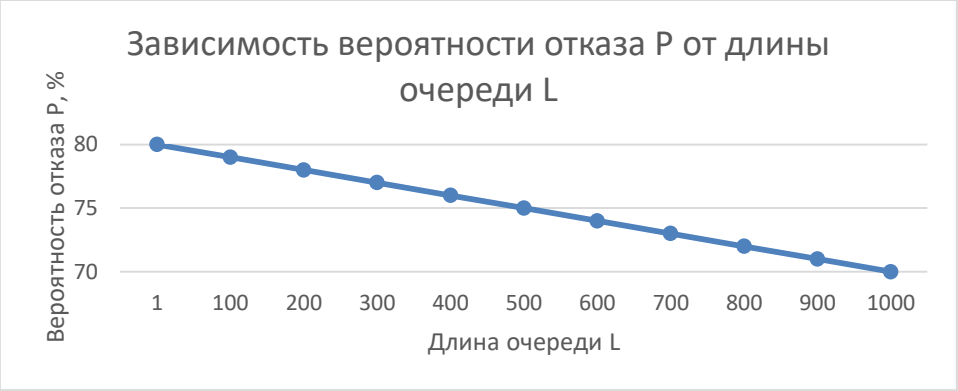

Рис.11. Зависимость вероятности отказа от длины очереди
Fig.11. Dependence of the probability of failure on the length of the queue

Вывод. На основании результатов проведённых исследований показана целесообразность применения имитационного моделирования методом Монте-Карло для оценки вероятности отказа сервера в условиях DDoS-атак. Был сделан вывод о том, что сервер может рассматриваться как СМО, однако поток поступающих заявок в условиях DDoS-атак не является пуассоновским, поэтому применение аналитических выражений для оценки вероятности отказа некорректно. Моделирование позволяет ЛПР оценить вероятность отказа сервера и принять организационные и технические меры для повышения уровня защищённости. Анализ результатов моделирования показал эффективность повышения производительности сервера путём увеличения каналов обслуживания. Таким образом, разработанная методика будет полезна при проведении аудита информационной безопасности организации для обоснования размера ее страховой премии в рамках страхования киберрисков.

Библиографический список:

1. Анализ существующих автоматизированных систем управления технологическим процессом [Электронный ресурс]. Режим доступа: https://cyberleninka.ru/article/n/analiz-suschestvuyuschih-avtomatizirovannyh-sistem-upravleniya-tehnologicheskim-protsessom/viewer.
2. Угроза DDoS-атак и неоднозначное к ним отношение [Электронный ресурс]. Режим доступа: https://www.kaspersky.ru/blog/ugroza-ddos-atak-i-neodnoznachnoe-k-nim-otnoshenie/3236/.
3. Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных" // СПС КонсультантПлюс.
4. Постановление Правительства РФ от 1 ноября 2012 г. N1119 г.Москва "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".
5. Постановление Правительства № 162 от 17.02.2018 г. «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».
6. Указ Президента РФ от 25.11.2017 N 569 "О внесении изменений в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента Российской Федерации от 16 августа 2004 г. N 1085.
7. NIST Special Publication 800-82 // Guide to Industrial Control Systems (ICS) [Электронный ресурс]. Режим доступа: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r1.pdf
8. Солнышкина И.В. Теория систем массового обслуживания: учеб. пособие / И.В. Солнышкина. – Комсомольск-на-Амуре :ФГБОУ ВПО «КнАГТУ», 2015. -76 с.
9. Теория массового обслуживания. Методические указания, учебная программа и задания для контрольных работ № 1, 2 для студентов заочной формы обучения специальности 071900 «Информационные системы в технике и технологиях». - Самара: СамГАПС, 2002.- 38с.
10. Лычкина Н.Н. Имитационное моделирование экономических процессов / Учебное пособие. — М.: Инфра-М, 2012. — 253 С.
11. Моделирование систем: учебное пособие / сост. Р. Г. Асулдаев. – Белгород, 2016. – 236 с.
12. Имитационное моделирование: учебное пособие/ Ю.А. Кораблев. Москва : КНОРУС, 2017. — 146 с.
13. Воеводин В.А., Черняев В.С. и Буренок Д.С. О применении имитационной модели для оценки вероятности отказа сервера в контексте DDoS-атак//Материалы 76-й Всероссийской конференции «Радиоэлектронные устройства и системы для инфокоммуникационных технологий», 2021, с. 390-393.
14. Lee J L and Hong C S 2013 Nonparametric Detection Methods against DDoS Attack Korean Journal of Applied Statistics vol 4 pp. 291-305.
15. Leian Chen, Xiaodong Wang 2020 Quickest attack detection in smart grid based on sequential Monte Carlo filtering» IET Smart Grid vol 3 pp. 686 – 696.

16. Мицель А.А., Грибанова Е.Б. Имитационное моделирование экономических процессов в Excel Томск: Изд-во ТУСУР, 2019. –115 с [Электронный ресурс].Режим доступа: https://asu.tusur.ru/learning/090303/d24/090303-d24-lect2.pdf
17. Воеводин В.А., Буренок Д.С. и Черняев В.С. 2021 Программа для оценки защищенности сервера от DDoS-атак Свидетельство об официальной регистрации компьютерной программы № 2021615403.

References:

1. Analysis of existing automated process control systems [Electronic resource]. Access mode: https://cyberleninka.ru/article/n/analiz-suschestvuyuschih-avtomatizirovannyh-sistem-upravleniya-tehnologicheskim-protsessom/viewer
2. The threat of DDoS attacks and ambiguous attitude to them [Electronic resource]. Access mode: https://www.kaspersky.ru/blog/ugroza-ddos-atak-i-neodnoznachnoe-k-nim-otnoshenie/3236/
3. Federal Law No. 152-FZ of 27.07.2006 "On personal data" // SPS ConsultantPlus.
4. Resolution of the Government of the Russian Federation of November 1, 2012 N 1119 Moscow "On approval of requirements for the protection of personal data during their processing in personal data information systems"
5. Government Resolution No. 162 of 17.02.2018 "On approval of the Rules for the Implementation of state Control in the Field of ensuring the security of Significant objects of critical information infrastructure of the Russian Federation"
6. Decree of the President of the Russian Federation of 25.11.2017 N 569 "On Amendments to the Regulations on the Federal Service for Technical and Export Control, approved by Decree of the President of the Russian Federation of August 16, 2004; 1085
7. NIST Special Publication 800-82. Guide to Industrial Control Systems (ICS) [Electronic resource]. Access mode: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r1.pdf
8. Solnyshkina I.V. Theory of queuing systems: textbook. Manual. Komsomolsk-on-Amur : FGBOU VPO "KnAGTU", 2015;76.[In Russ]
9. Queuing theory. Methodical instructions, curriculum and tasks for control works No. 1, 2 for correspondence students of the specialty 071900 "Information systems in engineering and technology". Samara: SamGAPS, 2002; 38.[In Russ]
10. Lychkina N.N. Simulation modeling of economic processes. Textbook. M.: Infra-M, 2012;253.[In Russ]
11. Modeling of systems: a textbook. comp. R. G. Asuldaev. Belgorod, 2016; 236. [In Russ]
12. Simulation modeling: textbook .Yu.A. Korablev. Moscow : KNORUS, 2017;146.[In Russ]
13. Voevodin V. A., Chernyaev V. S., Burenok D.S. On the use of a simulation model to assess the probability of server failure in the context of DDoS attacks // Proceedings of the 76th All-Russian Conference "Radioelectronic Devices and Systems for Infocommunication Technologies", 2021; 390-393. [In Russ]
14. Lee J L and Hong C S Nonparametric Detection Methods against DDoS Attack *Korean Journal of Applied Statistics* 2013; 4: 291-305.
15. Leian Chen, Xiaodong Wang. Quickest attack detection in smart grid based on sequential Monte Carlo filtering» IET Smart Grid 2020; 3: 686 – 696.
16. Micel` A.A., Gribanova E.B., Simulation of economic processes in Excel Tomsk: TUSUR Publishing House, 2019;115 [El.res.]. Access mode:https://asu.tusur.ru/learning/090303/d24/090303-d24-lect2.pdf
17. Voevodin V.A., Burenok D.S. i Chernyaev V.S. 2021 Program for evaluating server security from DDoS attacks Certificate of official registration of a computer program No. 2021615403.

Сведения об авторах:

Воеводин Владислав Александрович, кандидат технических наук, доцент, доцент кафедры информационной безопасности; vva541@mail.ru

Черняев Валентин Сергеевич, магистрант; sergeich1997@yandex.ru

Буренок Дмитрий Сергеевич, магистрант; corr.dmitry@yahoo.com

Виноградов Иван Вадимович, студент; ivanvinogradov1111@gmail.com

Information about authors:

Vladislav A. Voevodin, Cand. Sci. (Eng.), Assoc. Prof., Assoc. Prof., Department of Information Security; vva541@mail.ru

Valentin S. Chernyaev, Master's student; sergeich1997@yandex.ru

Dmitry S. Burenok, Master's student; corr.dmitry@yahoo.com

Ivan V. Vinogradov, Student; ivanvinogradov1111@gmail.com

Конфликт интересов/Conflict of interest.

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.

Поступила в редакцию/Received 18.01.2023.

Одобрена после рецензирования/ Reviced 22.02.2023.

Принята в печать/Accepted for publication 22.02.2023.