# МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ВЕКТОРА DDOS-АТАКИ НА СЕТЕВУЮ ИНФРАСТРУКТУРУ АСУ ТП С ИСПОЛЬЗОВАНИЕМ МЕТОДА ТОПОЛОГИЧЕСКОГО ПРЕОБРАЗОВАНИЯ СТОХАСТИЧЕСКИХ СЕТЕЙ[1]

***Богер А.М[2]., Соколов А.Н.[3]***

***Цель:*** *разработка математической модели вектора DDoS-атаки на сетевую инфраструктуру автоматизированной системы управления технологическим процессом для оценки среднего времени ее успешной реализации.*

***Метод исследования:*** *математическая модель вектора DDoS-атаки построена с использованием метода топологического преобразования стохастических сетей. Проверка полученных расчетных данных проведена с использованием экспериментального стенда, моделирующего работу сети автоматизированной системы управления технологическим процессом и находящегося под воздействием DDoS-атаки.*

***Полученный результат:*** *разработана модель нарушителя, организующего DDoS-атаку на сеть автоматизированной системы управления технологическим процессом, которая представляет собой последовательность действий нарушителя и создаваемых им процессов. Описаны зависимости процессов, создаваемых нарушителем, и вероятностные переходы между ними. Входные параметры математической модели определены в виде среднего времени продолжительности каждого из процессов. На основе процессов, описанных в модели нарушителя, составлена стохастическая сеть и построено характеристическое уравнение, позволяющее получить аппроксимированную функцию вектора DDoS-атаки. Выходные данные получены в виде среднего времени реализации успешной DDoS-атаки, а также зависимости вероятности успешности DDoS-атаки от ее продолжительности во времени. На стенде «Информационная безопасность в индустриальных системах» проведен ряд экспериментов, реализующих DDoS-атаку и позволяющих сделать заключение о соответствии реального времени реализации успешной DDoS-атаки рассчитанному с использованием построенной математической модели.*

***Научная новизна:*** *разработана математическая модель вектора DDoS-атаки на сетевую инфраструктуру автоматизированной системы управления технологическим процессом, отличающаяся применением метода топологического преобразования стохастической сети для построения модели нарушителя и оценки среднего времени успешной DDoS-атаки вне зависимости от ее вида и интенсивности. Разработанная модель отличается от существующих отсутствием необходимости учета определенного вида DDoS-атаки и ее интенсивности, а также наличием оценки продолжительности предварительных действий нарушителя.*

***Ключевые слова:*** *Автоматизированная система управления технологическим процессом (АСУ ТП), вектор атаки, защита информации, кибератака, математическая модель, модель нарушителя, топологическое преобразование стохастической сети.*

**DOI:**10.21681/2311-3456-2023-4-72-79

1 Исследование поддержано грантом Российского научного фонда (проект No 22-71-10095).

2 Богер Александр Максимович, преподаватель кафедры защиты информации ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)», г. Челябинск, Россия. E-mail: bogeram@susu.ru

3 Соколов Александр Николаевич, кандидат технических наук, доцент, заведующий кафедрой защиты информации ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)», г. Челябинск, Россия. E-mail: sokolovan@susu.ru

## Введение

Количество вредоносных воздействий, которые отмечаются в автоматизированных системах управления технологическими процессами (АСУ ТП), ежегодно увеличивается.[4] Это говорит о стойком интересе злоумышленников к подобным системам и тенденциям развития методов кибератак. При этом развитие систем противодействия атакам на АСУ ТП не всегда успевает за развитием методов кибератак [1]. В зоне риска находятся, в том числе программируемые логические контроллеры (ПЛК), поскольку, как правило, они являются частью промышленного цифрового оборудования, взаимодействующего с корпоративной сетью [2].

Одной из наиболее простых и эффективных кибератак является атака типа «Отказ в обслуживании» (Distributed Denial of Service, DDoS). DDoS-атаки относятся к наиболее распространенным атакам, нарушающим синхронизацию сетевых процессов. Количество DDoS атак непрерывно увеличивается, атаки становятся более интенсивными, продолжительными и включают большее количество целей.[5]

Известные модели DDoS-атак зачастую сложны и требуют знания особенностей конкретной DDoS-атаки и ее интенсивности [3, 4]. Нередко во входные показатели подобных математических моделей входит большое количество разнородных данных, многие из которых сложно задать с приемлемой точностью [5], либо требуют настройку и использование технологий искусственного интеллекта [6]. Это влияет на продолжительность расчетов и точность конечных результатов [7, 8].

Представленная модель не затрагивает особенности видов DDoS-атак, а опирается только на их влияние на целевой хост, которое характеризуется средним временем наступления отказа в обработке сигналов хостом.

Оценка времени наступления отказа в обработке, или по-другому, времени реализации успешной DDoS-атаки особенно важна для построения системы управления, т.к. большое количество обрабатываемых процессов, многие из которых осуществляются в опасных условиях, требуют точного и синхронизированного управления [9, 10]. Таким образом, даже малоинтенсивная DDoS-атака способна нарушить синхронизацию процессов в сети, а со временем и полностью прекратить коммуникацию, что может привести к значительным поломкам оборудования [11].

Поэтому системы защиты АСУ ТП необходимо проектировать с учетом времени реализации успешной DDoS-атаки для настройки их времени реакции. Значение среднего времени реализации успешной DDoS-атаки может быть использовано для оценки необходимого времени реакции систем защиты промышленных сетей и применения этого параметра во встроенных инструментах защиты информации. Если время реакции защитных систем и время на принятие необходимых мер меньше среднего времени реализации успешной атаки, то вероятность успеха и наличия ощутимых последствий DDoS-атаки значительно снижается.

На сегодняшний день ПЛК, как правило, обладают недостаточными встроенными инструментами защиты информации, либо не обладают ими вовсе [12], поэтому они крайне уязвимы к DDoS-атакам. Вследствие этого в технологические цифровые системы добавляются различные дополнительные системы защиты, в том числе адаптивные и интеллектуальные [13, 14].

Целью исследования является разработка математической модели вектора DDOS-атаки на ПЛК сети АСУ ТП, под которым понимается последовательность действий нарушителя, приводящая к получению несанкционированного доступа к целевой системе и приводящая к «отказу в обслуживании».

## Построение стохастической сети

Для реализации цели рассмотрена полноразмерная АСУ ТП, которая может включать в себя ПЛК, автоматизированные рабочие места на базе ПК (АРМ), серверную часть и различное коммутационное оборудование. Модель строится на основе стохастической сети [15] и позволяет оценить среднее время реализации успешной DDoS-атаки.[6]

Модель нарушителя предполагает, что при реализации DDOS-атаки:

1. Нарушитель создает процесс $A$ – запуска программного обеспечение для генерации запросов за время, которое определим как среднее время запуска $t_A$. Вероятность завершения процесса за время $t$

4 Ландшафт угроз для систем промышленной автоматизации. Статистика за первое полугодие 2022 [Электронный ресурс] // Kaspersky Industrial Control Systems Cyber Emergency Response Team: [сайт]. URL: https://ics-cert.kaspersky.ru/publications/reports/2022/09/08/threat-landscape-for-industrial-automation-systems-statistics-for-h1-2022/ – Дата обращения: 29.09.2022.

5 DDoS-атаки во втором квартале 2022 года [Электронный ресурс] // Securelist by Kapersky: [сайт]. URL: https://securelist.ru/ddos-attacks-in-q2-2022/105674/ – Дата обращения: 29.09.2022.

6 Привалов А. А. Метод топологического преобразования стохастических сетей и его использования для анализа систем связи ВМФ / А. А. Привалов. // Санкт-Петербург: ВМА, 2001. – 186

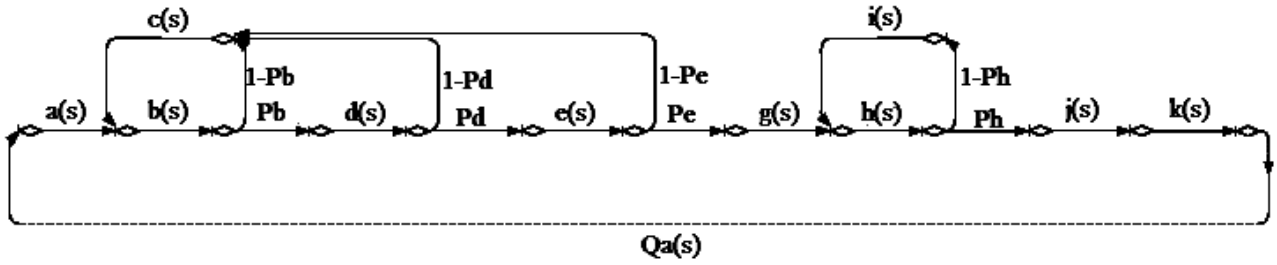


*Рис 1. Стохастическая сеть DDoS-атаки*

определим введением функции распределения вероятности $A(t)$.

2. Нарушитель сканирует сеть АСУ ТП с целью определения ее состава: рабочих элементов (процесс $B$), версий их ПО (процесс $D$) и состояния сетевых сервисов АСУ ТП (процесс $E$). Описанные действия нарушителя добиваются успеха, соответственно, с вероятностями $P_B$, $P_D$ и $P_E$ за средние времена $t_B$, $t_D$ и $t_E$. $B(t)$, $D(t)$ и $E(t)$ – соответствующие функции распределения вероятности завершения процессов $B$, $D$ и $E$ за время $t$. Указанные вероятности могут определяться с использованием базовых моделей угроз, либо выбираться из значений на интервале (0,1] с некоторым шагом.

3. Если какой-либо из процессов $B$, $D$ и $E$ завершается неудачей, нарушитель создает процесс $C$ – перезапуска программного обеспечения сканирования сети АСУ ТП с вероятностями $(1 - P_B)$, $(1 - P_D)$ и $(1 - P_E)$ за среднее время $t_C$, определяемое $C(t)$ – функцией распределения вероятности завершения процесса $C$ за время $t$.

4. Нарушитель анализирует собранные данные с целью поиска уязвимостей оборудования (процесс $G$) за среднее время $t_G$ с $G(t)$ – функцией распределения вероятности завершения процесса $G$ за время $t$.

5. При успешном завершении процесса $G$ нарушитель создает процесс $H$ – подключение к целевому хосту АСУ ТП. Подключение происходит за среднее время $t_H$ с $H(t)$ – функцией распределения вероятности завершения процесса $H$ за время $t$. Возможность подключения к атакуемому хосту характеризуется вероятностью $P_H$. Вероятность может определяться с использованием базовых моделей угроз, либо приравниваться к значениям на интервале (0,1] с некоторым шагом.

6. Если процесс подключения $H$ не завершается успехом, нарушитель инициирует процесс $I$ – сброс и подготовка к новой попытке с вероятностью $(1\text{-}P_H)$ за среднее время $t_I$ с $I(t)$ – функцией распределения вероятности завершения процесса $I$ за время $t$.

7. Если процесс $H$ заканчивается успешно, инициируется процесс $J$, при котором нарушитель получает подтверждение об подключении за среднее время $t_J$ с $J(t)$ – функцией распределения вероятности завершения процесса J за время $t$.

8. При успешной реализации всех предшествующих процессов нарушитель инициирует процесс K – непосредственную DDoS-атаку, отправляя запросы на атакуемый хост. Результат атаки проявляется за среднее время $t_K$ с $K(t)$ – функцией распределения вероятности завершения процесса J за время $t$.

С учетом вышеописанных зависимостей, определим среднее время и функцию распределения $F(t)$ времени реализации успешной DDoS-атаки. Предполагается, что все используемые вероятности принимают одинаковые значение $P$ на интервале [0,7 , 1] с шагом 0,1:

$$P_B=P_D=P_E=P_H=P.$$

Описанные процессы выполняются на цифровом оборудовании и их поведение склонно показывать, что с большей вероятностью они закончатся за малый промежуток времени, чем за больший, следовательно, все функции распределения представлены в виде вариаций показательного распределения, т.е. имеющих вид $y(t)= 1 - e^{\lambda t}$.

Для построения стохастической сети проведены операции свертки с функциями распределения, приведя их к виду $a(s)$, $b(s)$, $c(s)$, $d(s)$, $e(s)$, $g(s)$, $h(s)$, $i(s)$, $j(s)$, $k(s)$. Для этого использовано преобразование Лапласа-Стилтьеса:

$$y(s) = \int_0^{+\infty} e^{-st} d(Y(t)) = \frac{\lambda}{\lambda + s}, \quad (1)$$

где $\lambda=1/t$ – параметр показательного распределения.

На основании введенных функций и зависимостей между ними составлена стохастическая сеть, которая замыкается фиктивной ветвью $Q_a(S)=1/Q(s)$ (рис. 1).

## Топологическое преобразование стохастической сети вектора DDoS-атаки

Для стохастической сети определена характеристическая функция, включающая следующие петли:

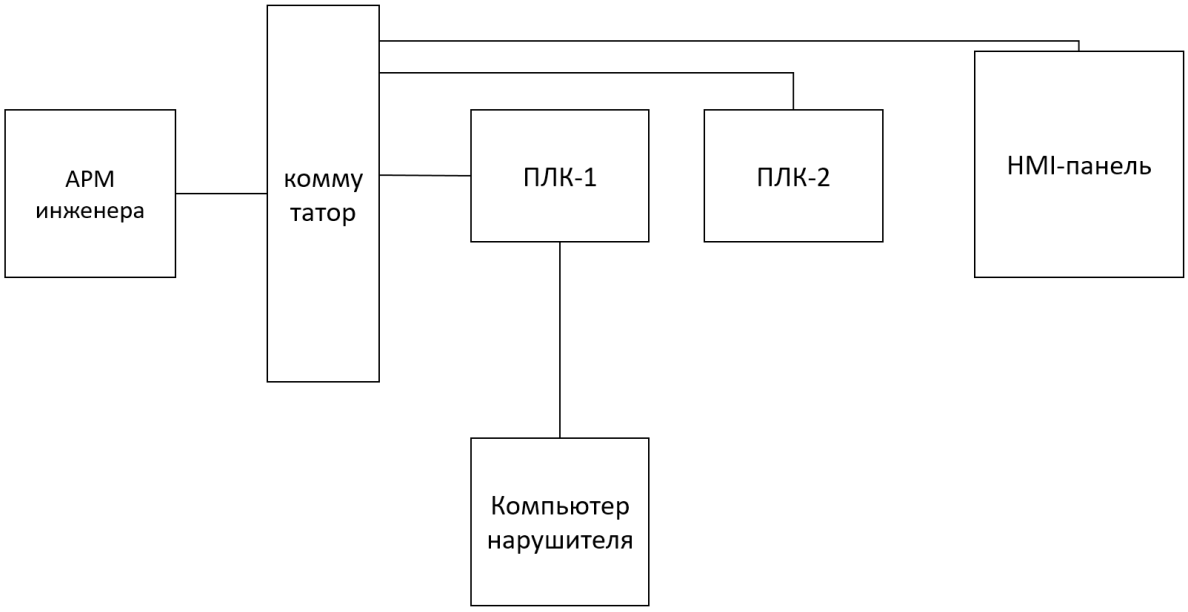


*Рис.2. Структурная схема лабораторного стенда «Информационная безопасность в индустриальных системах»*

Петли первого порядка:

$-b(s)*(1-P)*c(s);$

$-b(s)*d(s)*P*(1-P)*c(s);$

$-b(s)*d(s)*e(s)*P^2*(1-P)*c(s);$

$-h(s)*(1-P)*i(s).$

Петли второго порядка:

$-b(s)*(1-P)^2*c(s)*h(s)*i(s);$

$-b(s)*d(s)*P*(1-P)^2*c(s)*h(s)*i(s);$

$-b(s)*d(s)*e(s)*P^2*(1-P)^2*c(s)*h(s)* *i(s).$

Для построения эквивалентной функции стохастической сети использовано уравнение Мейсона:

$$H = 1 + \sum_{N=1}^{l} (-1)^l Q_l(s) = 0, \quad (2)$$

где $Q_l(s)$ – эквивалентные функции петель порядка l. Таким образом, эквивалентная функция $Q(s,P)$ имеет вид: $Q(s,P)=Q_x/Q_y$, где:

$$Q_x = a(s)*b(s)*d(s)*e(s)*g(s)*h(s)* *j(s)*k(s)*P^4, \quad (3)$$

$$Q_y = 1-b(s)*(1-P)*c(s)*(1+d(s)*P* *(1+e(s)*P))+h(s)* *(1-P)*i(s)*(-1*b(s)*(1-P)* *c(s)*(1+d(s)*P*(1+e(s)*P))) \quad (4)$$

Используя метод двухмоментной аппроксимации и характеристическую функцию $Q(s,P)$, определим математическое ожидание среднего времени атаки и его дисперсию:

$$\bar{t}(P) = M_1(s,P) = -\frac{d}{ds}\left[\frac{Q(s,P)}{Q(s=0,P)}\right]_{s=0}, \quad (5)$$

$$D(\bar{t}) = M_2(s,P) - M_1^2(s,P) = , \quad (6)$$

$$= \frac{d^2}{ds^2}\left[\frac{Q(s,P)}{Q(s=0,P)}\right]_{s=0} - \left(-\frac{d}{ds}\left[\frac{Q(s,P)}{Q(s=0,P)}\right]_{s=0}\right)^2$$

где $M_1$, $M_2$ – моменты случайного времени процесса DDoS-атаки.

Найденные величины позволяют определить функцию распределения вероятности успешности DDoS-атаки, с помощью использования неполной гамма-функции

$$F(t) = \int_0^t \frac{\mu^\alpha}{\Gamma(\alpha)} t^{\alpha-1} e^{-\mu t}, \quad (7)$$

где $\pm = \frac{(\bar{t}(P))^2}{D(\bar{t})}$ – параметр формы, $\mu = \frac{\bar{t}(P)}{D(\bar{t})}$ – параметр масштаба.

## Экспериментальные результаты

Для проверки адекватности построенной математической модели проведен ряд экспериментов на лабораторном стенде «Информационная безопасность в индустриальных системах», включающем:

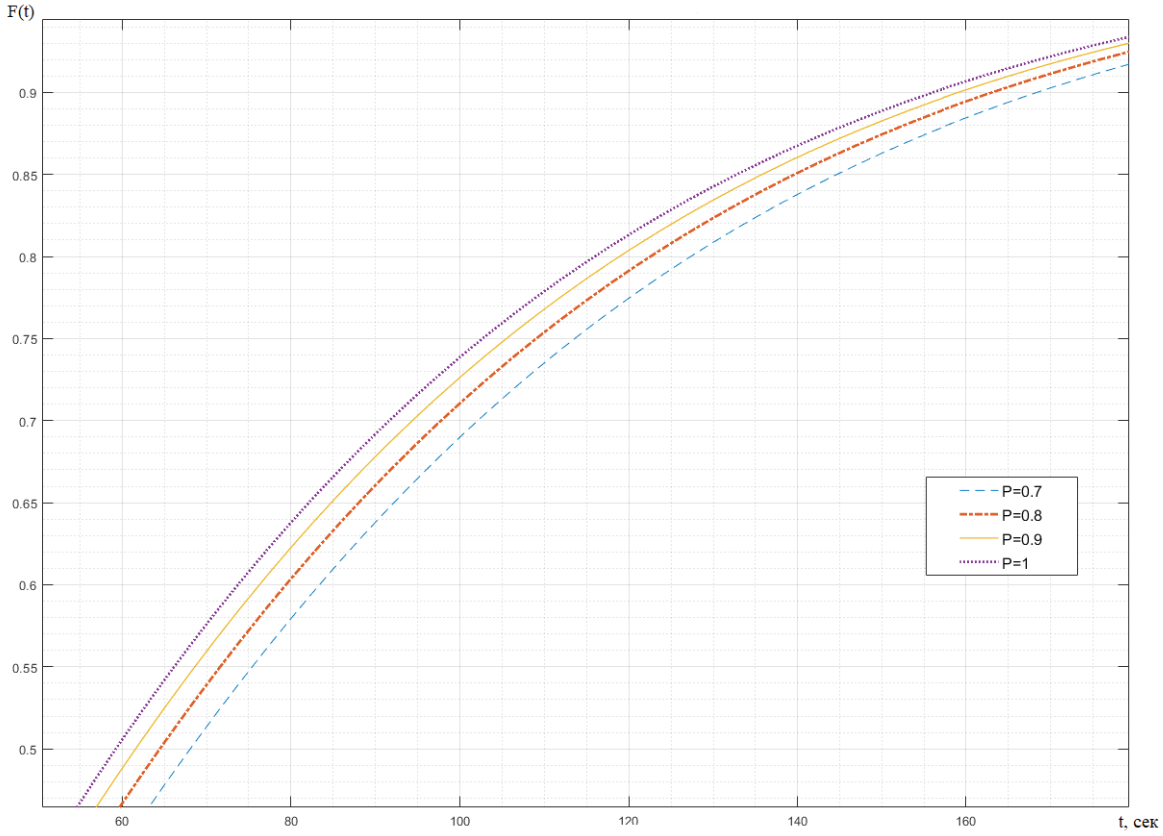


*Рис. 3. Зависимость вероятности реализации успешной атаки F(t) для разных значений вероятности P успешного завершения отдельного процесса*

— ПЛК-1: Siemens-1512;
— ПЛК-2: Siemens-1510;
— Коммутатор Scalance XC208;
— АРМ инженера, содержащая ПО для программирования ПЛК;
— HMI- панель для визуализации и управления.

На ПЛК-1 и ПЛК-2 загружена программа, эмулирующая металлонарезной станок. Для создания распределенного DoS-воздействия к стенду подключен ноутбук, исполняющий роль компьютера нарушителя и/или закладного устройства (первый поток запросов, рис. 2). В половине экспериментов ноутбук подключался к ПЛК, в остальных случаях – к коммутатору. Второй поток запросов атаки генерировался на АРМ инженера (имитация внутренней атаки). В качестве метода DoS-воздействия выбраны UDP-запросы по IP-адресу ПЛК-1. Активность воздействия – 100000 запросов в секунду с каждого из двух устройств.

В проведенном эксперименте условному нарушителю известны архитектура сети и уязвимости ПЛК, запущена программа генерации запросов, и настроено подключение к атакуемому хосту. Следовательно, временные промежутки запуска ПО, подключения к сети, анализа сети и уязвимостей оборудования равны нулю. Время инициализации и перезапуска атаки – 10 секунд, время отклика – 5 секунд, приблизительное время возникновения эффектов на данном типе ПЛК при прямом подключении – около минуты:

$$t_A=0\ \text{с} \qquad t_G=0\ \text{с}$$
$$t_B=0\ \text{с} \qquad t_H=10\ \text{с}$$
$$t_C=0\ \text{с} \qquad t_I=6\ \text{с}$$
$$t_D=0\ \text{с} \qquad t_J=10\ \text{с}$$
$$t_E=0\ \text{с} \qquad t_K=60\ \text{с}$$

Несколько запусков LOIC показали, что в течение 7 – 10 секунд после начала DoS-воздействия пропадала связь ПЛК с отслеживающим модулем. Полноценное прекращение сетевой передачи данных происходило приблизительно через 70 – 80 секунд. В результате эксперимента были получены следующие временные значения, представленные в таблице 1.

*Таблица 1*

*Результаты экспериментов*

| Эксперимент | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | среднее |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Время появления первых эффектов, с | 9,71 | 7,93 | 8,71 | 9,77 | 7,75 | 8,55 | 9,15 | 8,06 | 8,90 | 7,66 | 8,62 |
| Время окончательного обрыва связи, с | 84 | 79 | 70 | 77 | 82 | 85 | 81 | 70 | 73 | 83 | 78,4 |

На рис. 3 приведены функции распределения, вычисленные по формуле (7) при заданных входных параметрах. Расчетное время реализации успешной DDoS-атаки в условиях эксперимента составило 75 ± 3 с, что соответствует значениям, полученным в ходе эксперимента, где среднее время прекращения ответа хоста составило около 75 секунд.

## Вывод

Результаты, полученные расчетным путем с использованием разработанной математической модели вектора DDoS-атаки, соответствуют экспериментальным данным. Предложенную модель можно использовать для прогноза времени реализации успешной атаки, что позволяет оценивать необходимое время реакции систем защиты. Если время реакции систем защиты АСУ ТП и время выполнения ими защитных действий меньше, чем рассчитанное среднее время реализации успешной DDoS-атаки, то вероятность того, что атака будет обнаружена, а необходимые защитные меры своевременно приняты, значительно возрастает, что существенно уменьшает вероятность возникновения значительных последствий от DDoS-атаки. Функция распределения вероятности успешности атаки от времени может быть использована в качестве параметра в других, более узкоспециализированных математических моделях оценки успешности кибератак, либо в качестве источника данных для дополнительного анализа поведения DDoS-атаки.

## Литература


1. Абдулин А. А. Исследование программных решений для обеспечения информационной безопасности промышленных сетей автоматизированных систем управления технологическими процессами / А. А. Абдулин, А. Н. Соколов // Вестник УрФО. Безопасность в информационной сфере. – 2021. – № 1(39). – С. 43–53.
2. Соколов А. Н. Разработка моделей и методов раннего обнаружения кибератак на объекты энергетики металлургического предприятия / А. Н. Соколов, А. Н. Рагозин, А. Е. Баринов [и др.] // Вестник УрФО. Безопасность в информационной сфере. – 2021. – № 3(41). – С. 65–87.
3. Simona Ramanauskaitė, Antanas Cenys. Composite Dos Attack Model// Mokslas - Lietuvos ateitis – 2022.–Т. 4. – С. 20–26. – DOI:10.3846/mla.2022.05.
4. Juan Fernando Balarezo, Song Wang, Karina Gomez Chavez, Akram Al-Hourani, Sithamparanathan Kandeepan. A survey on DoS/DDoS attacks mathematical modelling for traditional, SDN and virtual networks// Engineering Science and Technology, an International Journal. – 2022. – Т. 31. – DOI: 10.1016/j.jestch.2021.09.011.
5. Yang H. Evaluation of DDOS Attack Degree Based on GRA-TOPSIS Model. / H. Yang, R. Jiang, C. Zhao, A. Li // 2019 International Conference on Smart Grid and Electrical Automation (ICSGEA). – 2019. – С. 547-552. – DOI: 10.1109/ICSGEA.2019.00129.
6. Guo W. The Evaluation of DDoS Attack Effect Based on Neural Network / Guo, Wei & Qiu, Han & Liu, Zimian & Zhu, Junhu & Wang, Qingxian. // Security and Communication Networks. – 2022. – Т. 6. – С. 1-16. –DOI: 10.1155/2022/5166323.
7. Khundrakpam Johnson Singh, Tanmay De. Mathematical modelling of DDoS attack and detection using correlation// Journal of Cyber Security Technology. – 2019. – С.175-186. – DOI: 10.1080/23742917.2019.1384213
8. Bimal Kumar Mishra, Ajit Kumar Keshri, Dheeresh Kumar Mallick, Binay Kumar Mishra. Mathematical model on distributed denial of service attack through Internet of things in a network// Nonlinear Engineering.– 2019. – Т. 8. – #1.– С. 486-495. –DOI:10.1515/nleng-2017-0094
9. Слинин, А. В. Интеллектуальная система оценки рисков информационной безопасности АСУ ТП объекта нефтедобычи / А. В. Слинин, В. И. Васильев // Информационные технологии интеллектуальной поддержки принятия решений : Труды VII Всероссийской научной конференции (с приглашением зарубежных ученых). В 3-х томах, Уфа, 28–30 мая 2019 года. Том 1. – Уфа: ГОУ ВПО “Уфимский государственный авиационный технический университет”, 2019. – С. 207-214.
10. Римша, А. С. Анализ средств обеспечения информационной безопасности АСУ ТП газодобывающих предприятий / А. С. Римша, К. С. Римша // Прикаспийский журнал: управление и высокие технологии. – 2019. – № 3(47). – С. 102-121. – DOI 10.21672/2074-1707.2019.47.3.102-121

11. Богер, А. М. Оценка воздействий DOS-атаки на трафик обмена данными между программируемыми логическими контроллерами SIMATIC 1510 и SIMATIC 1512 / А. М. Богер, А. Н. Соколов, И. А. Морозов // Вестник УрФО. Безопасность в информационной сфере. – 2022. – № 4(46). – С. 88-96. – DOI 10.14529/secur220410
12. Wang Z. A Survey on Programmable Logic Controller Vulnerabilities, Attacks, Detections, and Forensics/ Z. Wang, Y. Zhang, Y. Chen [и др.]// Processes. – 2023. – Т. 11. – № 918. – DOI: 10.3390/pr11030918
13. Басан А.С. Адаптивная система защиты сенсорных сетей от активных атак/ А.С. Басан, Е.С. Басан, О.Ю. Пескова [и др.] // Вопросы кибербезопасности. – 2022. – № 6(52)– С. 22–39. – DOI :10.21681/2311-3456-2022-6-22-39
14. Котенко И.В. Подсистема предупреждения компьютерных атак на объекты критической информационной инфраструктуры: анализ функционирования и реализации / И.В. Котенко, И.Б. Саенко, Р.И. Захарченко, Д.В. Величко // Вопросы кибербезопасности. – 2023. – № 1(53)– С. 13–27. – DOI : 10.21681/2311-3456-2023-1-13-27
15. Бекбаев Г. А. Подход к моделированию процесса DDoS-атаки на информационно-телекоммуникационную сеть железнодорожного транспорта/ Г. А. Бекбаев, А. А. Привалов, О. А. Турдиев// Вестник СамГУПС. – 2018. – № 1(39). – С. 100-108.

# MATHEMATICAL MODEL OF THE VECTOR OF A DDOS ATTACK ON THE ICS USING THE METHOD OF TOPOLOGICAL TRANSFORMATION OF STOCHASTIC NETWORKS

***Boger A. M.[7], Sokolov A. N.[8]***

***Aim:*** *development of a mathematical model of the vector of a DDoS attack on the network infrastructure of an Industrial Control System to estimate the average time of its successful implementation.*

***Research method:*** *a mathematical model of the DDoS attack vector was built using the method of topological transformation of stochastic networks. The verification of the obtained calculated data was carried out using an experimental stand that simulates the operation of a network of an Industrial Control System and is under the influence of a DDoS attack.*

***Result:*** *a model of an intruder that organizes a DDoS attack on the network of an Industrial Control System has been developed, which is a sequence of actions of the intruder and the processes he creates. The dependencies of the processes created by the intruder and the probabilistic transitions between them are described. The input parameters of the mathematical model are defined as the average duration of each of the processes. Based on the processes described in the intruder's model, a stochastic network was compiled, and a characteristic equation was constructed that allows obtaining an approximate function of the DDoS attack vector. The output data is obtained in the form of the average time of a successful DDoS attack, as well as the dependence of the probability of a successful DDoS attack on its duration in time. At the stand "Information security in industrial systems" several experiments were carried out that implement a DDoS attack and allow us to conclude that the real time of a successful DDoS attack is consistent with the one calculated using the constructed mathematical model.*

***Scientific novelty*** *of the research: a mathematical model of the vector of a DDoS attack on the network infrastructure of an Industrial Control System has been developed, which is distinguished using the method of topological transformation of a stochastic network to build an intruder model and estimate the average time of a successful DDoS attack, regardless of its type and intensity. The developed model differs from the existing ones by the absence of the need to consider a certain type of DDoS attack and its intensity, as well as by the presence of an estimate of the duration of the intruder's preliminary actions.*

***Keywords:*** *Industrial Control System (ICS), information protection, cyberattack, mathematical model, intruder model, topological transformation of a stochastic network.*

7 Aleksandr M. Boger, Lecturer of Department of Information Security, Federal State Autonomous Educational Institution of Higher Education "South Ural State University (national research university)". Chelyabinsk, Russia, E-mail: bogeram@susu.ru

8 Alexander N. Sokolov, Ph.D., Associate Professor, Head of Department of Information Security, Federal State Autonomous Educational Institution of Higher Education «South Ural State University (national research university)»., Chelyabinsk, Russia. E-mail: sokolovan@susu.ru

## References


1. Abdulin A. A. Issledovanie programmnyh reshenij dlya obespecheniya informacionnoj bezopasnosti promyshlennyh setej avtomatizirovannyh sistem upravleniya tekhnologicheskimi processami / A. A. Abdulin, A. N. Sokolov // Vestnik UrFO. Bezopasnost' v informacionnoj sfere. – 2021. – № 1(39). – S. 43–53.
2. Sokolov A. N. Razrabotka modelej i metodov rannego obnaruzheniya kiberatak na ob"ekty energetiki metallurgicheskogo predpriyatiya / A. N. Sokolov, A. N. Ragozin, A. E. Barinov [i dr.] // Vestnik UrFO. Bezopasnost' v informacionnoj sfere. – 2021. – № 3(41). – S. 65–87.
3. Simona Ramanauskaitė, Antanas Cenys. Composite Dos Attack Model// Mokslas - Lietuvos ateitis – 2022.–T. 4. – S. 20–26. – DOI:10.3846/mla.2022.05.
4. Juan Fernando Balarezo, Song Wang, Karina Gomez Chavez, Akram Al-Hourani, Sithamparanathan Kandeepan. A survey on DoS/DDoS attacks mathematical modelling for traditional, SDN and virtual networks// Engineering Science and Technology, an International Journal. – 2022. – T. 31. – DOI: 10.1016/j.jestch.2021.09.011.
5. Yang H. Evaluation of DDOS Attack Degree Based on GRA-TOPSIS Model. / H. Yang, R. Jiang, C. Zhao, A. Li // 2019 International Conference on Smart Grid and Electrical Automation (ICSGEA). – 2019. – C. 547-552. – DOI: 10.1109/ICSGEA.2019.00129.
6. Guo W. The Evaluation of DDoS Attack Effect Based on Neural Network / Guo, Wei & Qiu, Han & Liu, Zimian & Zhu, Junhu & Wang, Qingxian. // Security and Communication Networks. – 2022. – T. 6. – C. 1-16. –DOI: 10.1155/2022/5166323.
7. Khundrakpam Johnson Singh, Tanmay De. Mathematical modelling of DDoS attack and detection using correlation// Journal of Cyber Security Technology. – 2019. – S.175-186. – DOI: 10.1080/23742917.2019.1384213
8. Bimal Kumar Mishra, Ajit Kumar Keshri, Dheeresh Kumar Mallick, Binay Kumar Mishra. Mathematical model on distributed denial of service attack through Internet of things in a network// Nonlinear Engineering.– 2019. – T. 8. – #1.– S. 486-495. –DOI:10.1515/nleng-2017-0094
9. Slinin, A. V. Intellektual'naya sistema ocenki riskov informacionnoj bezopasnosti ASU TP ob"ekta neftedobychi / A. V. Slinin, V. I. Vasil'ev // Informacionnye tekhnologii intellektual'noj podderzhki prinyatiya reshenij : Trudy VII Vserossijskoj nauchnoj konferencii (s priglasheniem zarubezhnyh uchenyh). V 3-h tomah, Ufa, 28–30 maya 2019 goda. Tom 1. – Ufa: GOU VPO "Ufimskij gosudarstvennyj aviacionnyj tekhnicheskij universitet", 2019. – S. 207-214.
10. Rimsha, A. S. Analiz sredstv obespecheniya informacionnoj bezopasnosti ASU TP gazodobyvayushchih predpriyatij / A. S. Rimsha, K. S. Rimsha // Prikaspijskij zhurnal: upravlenie i vysokie tekhnologii. – 2019. – № 3(47). – S. 102-121. DOI: 10.21672/2074-1707.2019.47.3.102-121
11. Boger, A. M. Ocenka vozdejstvij DOS-ataki na trafik obmena dannymi mezhdu programmiruemymi logicheskimi kontrollerami SIMATIC 1510 i SIMATIC 1512 / A. M. Boger, A. N. Sokolov, I. A. Morozov // Vestnik UrFO. Bezopasnost' v informacionnoj sfere. – 2022. – № 4(46). – S. 88-96. – DOI 10.14529/secur220410
12. Wang Z. A Survey on Programmable Logic Controller Vulnerabilities, Attacks, Detections, and Forensics/ Z. Wang, Y. Zhang, Y. Chen [i dr.]// Processes. – 2023. – T. 11. – № 918. – DOI: 10.3390/pr11030918
13. Basan A.S. Adaptivnaya sistema zashchity sensornyh setej ot aktivnyh atak/ A.S. Basan, E.S. Basan, O.YU. Peskova [i dr.] // Voprosy kiberbezopasnosti. – 2022. – № 6(52)– S. 22–39. – DOI :10.21681/2311-3456-2022-6-22-39
14. Kotenko I.V. Podsistema preduprezhdeniya komp'yuternyh atak na ob"ekty kriticheskoj informacionnoj infrastruktury: analiz funkcionirovaniya i realizacii / I.V. Kotenko, I.B. Saenko, R.I. Zaharchenko, D.V. Velichko // Voprosy kiberbezopasnosti. – 2023. – № 1(53)– S. 13–27. – DOI : 10.21681/2311-3456-2023-1-13-27
15. Bekbaev G. A. Podhod k modelirovaniyu processa DDoS-ataki na informacionno-telekommunikacionnuyu set' zheleznodorozhnogo transporta/ G. A. Bekbaev, A. A. Privalov, O. A. Turdiev// Vestnik SamGUPS. – 2018. – № 1(39). – S. 100-108.