Электричество, 2022, № 3, с. 49–57 *DOI:10.24160/0013-5380-2022-3-49-57*

Противодействие кибератакам типа отказ в обслуживании (*DDoS*-атакам) в энергетическом секторе

ДМИТРИЕВ Д.В., ЛЯХМАНОВ Д.А., СОКОЛОВА Э.С.
НГТУ им. Р.Е. Алексеева, Нижний Новгород, Россия

Цифровизация инфраструктур с использованием информационных технологий для эффективного интеллектуального управления энергосистемами и низкий уровень их информационной защищенности приводят к увеличению числа кибератак в энергетической сфере. При этом энергетические объекты являются критически важными и нарушение их функционирования влияет на национальную безопасность. Уже на правительственном уровне многих государств кибератаки на объекты инфраструктуры энергетики воспринимаются как реальные угрозы, приводящие к нарушениям функционирования объектов топливно-энергетического комплекса. Наблюдается устойчивый рост распределенных кибератак типа отказ в обслуживании (DDoS-атак), направленных на энергетические объекты. Атакам подвергаются системы автоматизации зданий и управления электроэнергией, call-центры энергетических компаний, в результате чего нарушается энергоснабжение целых райнов на длительное время. В настоящее время не существует надежных универсальных технологий, блокирующих DDoS-атаки. В работе представлен метод противодействия DDoS-атакам в энергетических системах на основе несемантической фильтрации трафика. Представлен новый подход противодействия DDoS-атакам, защищающий серверы и полосу пропускания трафика, основанный на взаимодействии пользователей с серверным оборудованием посредством динамической смены IP-адресов атакуемых ресурсов по формируемому псевдослучайно расписанию. Разработанная технология фильтрации сетевого трафика позволяет противодействовать распределенным DDoS-атакам, снижая интенсивность атак на 92 % при потере легитимных пакетов, неизбежной при реализации любой технологии противодействия DDoS, менее 2 %.

Ключевые слова: *умная энергетика, цифровизация, распределенные атаки, кибербезопасность*

Процесс цифровизации общества предполагает массовое внедрение киберфизических систем в реальную экономику, промышленные системы управления и производственные процессы. Процесс внедрения идет не линейными, а экспоненциальными темпами. Коснулось это и электроэнергетики. В ходе цифровизации электроэнергетической системы за счет использования эффективного анализа данных в реальном времени повышается энергоэффективность и оптимизируется управление энергетическими потоками в цепочке поставок энергии [1, 2]. Процесс управления и мониторинга электроэнергетической системой становится гибким и эффективным [3]. Использование датчиков и коммуникационных технологий (особенно беспроводных) позволяет считывать и передавать данные в реальном времени в вычислительные центры, что обеспечивает корректную обработку данных и принятие оптимальных управляющих решений энергосетью в режиме реального времени с применением интеллектуальных алгоритмов анализа данных [4]. При этом осуществляется переход от централизованной к распределенной энергетической системе. Это приводит к тому, что цифровое пространство электроэнергетики становится более открытым и, соответственно, более уязвимым для информационных атак как снаружи, так и изнутри управляющих информационных систем [5].

В современном цифровом мире постоянно растет актуальность вопросов кибербезопасности в электроэнергетике в связи с увеличением числа кибератак. Открытость информационного пространства, тесная связь интернета с реальной экономикой, промышленными системами управления, производственными процессами приводит к росту уязвимостей, имеющих высокую степень риска. Одной из самых распространенных кибератак является распределенная атака типа «отказ в обслуживании» (*DDoS*) [6]. Следует отметить, что воздействие *DDoS*-атак на цифровую инфраструктуру электроэнергетики может привести к самым серьезным последствиям вполне физического характера (выход из строя оборудования цифровых подстанций, массовое отключение электроэнергии у потребителей и т.п.). Зависимость процессов энергокомпаний от интернет-коммуникаций для передачи информации, реализации управления работой объектов в случае направленной *DDoS*-атаки приводит к полной остановке рабочего процесса из-за отказа сети до окончания атаки или успешной блокировки нежелательного трафика. Проблеме угрозы кибератак на энергосистемы по-

священ ряд отечественных и зарубежных работ [7–11] Примечательно то, что *DDoS*-атака является универсальным инструментом кибервредителей, от которого пока нет надежного и эффективного способа защиты цифровой инфраструктуры. По данным аналитических отчетов *Qrator Labs* ежегодно количество *DDoS*-атак увеличивается на четверть [12]. 2019–2021 гг. не стали исключением. Под ударом находятся не только информационные сетевые ресурсы энергокомпаний, но и физические объекты электроэнергетики повышенной степени ответственности. При атаке на несколько подстанций высокого и среднего напряжений могут выводиться из строя целые районные энергосистемы [13].

Традиционные методы снижения риска угроз информационной безопасности, такие как шифрование передаваемой информации [14], интеллектуальная фильтрация трафика и распределенное управление энергосистемой на разных уровнях [15], позволяют усложнить перехват данных, но малоэффективны при *DDoS*-атаках.

Для снижения эффективности *DDoS*-атак на цифровые ресурсы в большинстве случаев используется два подхода. Первый заключается в географическом распределении и зеркализации цифрового ресурса. При этом в случае атаки выходит из строя только небольшой сегмент инфраструктуры цифрового ресурса. Второй вариант подразумевает наращивание средств обработки сетевых запросов и снижение «вычислительной стоимости» обработки одного запроса. Данный подход способен сделать информационную систему более устойчивой к воздействиям *DDoS*-атак, но обладает серьезными недостатками, среди которых высокая стоимость и отсутствие защищенности от всех типов *DDoS*-атак.

Применение описанных методов в отношении энергосистем в большинстве случаев не дает нужного эффекта, так как выход из строя даже небольшого управляющего сегмента энергосистемы может привести к аварийным ситуациям, а наращивание вычислительной инфраструктуры не является рациональным финансово. Также их применение может значительно увеличивать нагрузку на цифровую инфраструктуру электроэнергетики, что усложняет процесс цифровизации электрических сетей. Следует отметить, что обеспечение кибербезопасности не должно препятствовать цифровизации.

Для оптимального управления энергетическими потоками в цепочке поставок энергии в последнее время в распределительных сетях сложной конфигурации эффективно используются интеллектуальные регуляторы напряжения и потоков мощности [16], предполагающие наличие каналов связи информационного обмена на разных уровнях взаимодействия. Эти каналы связи организуются между самими интеллектуальными регуляторами, между интеллектуальными регуляторами и узлами распределительной электрической сети, интеллектуальными регуляторами и сетью Интернет. В случае наличия взаимодействия с глобальной сетью Интернет возникает повышенная уязвимость информационных систем в целом, в том числе и от *DDoS*-атак.

Современные технологии проведения *DDoS*-атак таковы, что инструменты для организации атак представляют собой высокоинтеллектуальные программные продукты, использующие последние достижения в сфере информационных технологий. Целью атакующих элементов при этом является максимально полная имитация легитимного трафика от реальных устройств или пользователей. В случае распределительной электрической сети это может быть имитация узла генерации, транспортного узла просьюмера, узла нагрузки обычного потребителя или даже узла активного потребителя электроэнергии. Все это снижает эффективность современных методов противодействия, основанных на интеллектуальной фильтрации трафика, и требует развития методов, основанных на совершенно иных подходах противодействия. Одно из решений в области информационной безопасности, призванных обеспечить высокую защищенность в распределительных электрических сетях сложной конфигурации, заключается во внедрении решений противодействия *DDoS*-атакам, основанных на динамической смене *IP*-адресов защищаемых ресурсов. Такой подход позволяет снизить эффективность распределенных атак путем полной фильтрации трафика, основанной на «плавающей» маршрутизации сетевых пакетов.

Методология защиты. Для повышения эффективности противодействия *DDoS*-атакам в распределительных электрических сетях сложной конфигурации предложена методика многоагентного моделирования защиты от атак. В результате системного анализа задачи моделирования защиты от *DDoS*-атак, включающего анализ методов работы агентов в команде, анализ существующих сегодня *DDoS*-атак и инструментов противодействия им, предложен подход, включающий моделирование команды атакующей стороны (эмулятор паразитного трафика), моделирование инструмента защиты и моделирование их взаимодействия. Модели представляют собой набор параметров, основных методов и правил взаимодействия в ходе выполнения *DDoS*-атак и защиты от них.

На текущий момент взаимодействие моделей атаки и защиты *DDoS* реализовано на уровне сети Интернет, но возможно и на уровне взаимодействия по проприетарным протоколам между узлами распределительной электрической сети с интеллектуальными регуляторами.

В основу предлагаемого метода защиты распределенных электрических сетей от *DDoS*-атак положен принцип снижения вычислительных мощностей, затрачиваемых на обработку приходящих сетевых пакетов. Снижение вычислительной «стоимости» каждого сетевого пакета достигается введением в процесс их обработки легковесных методов распознавания вредо-

носного трафика, предшествующих основным ресурсоемким методам обработки [17]. В рамках данной статьи предлагается метод предобработки, основанный на динамической смене *IP*-адресов и «плавающей» маршрутизации сетевых пакетов.

Принцип динамической смены *IP*-адресов заключается в смене *IP*-адреса принимающей стороны (узлы нагрузки и интеллектуальные регуляторы) по расписанию, известному только авторизованным пользователям. При этом неавторизованные клиенты, не имея достоверной информации о расписании смены адресов, посылают сетевые пакеты на *IP*-адреса приемников, не соответствующие расписанию. Такие сетевые пакеты распознаются и удаляются файрволами информационной сети. Физической смены *IP*-адреса принимающей стороны в данном случае не происходит. Достигается это путем наличия в информационной системе нескольких принимающих маршрутизаторов с функцией фильтрации, имеющих *IP*-адрес. Процесс смены *IP*-адреса принимающей стороны равносилен определению маршрута и принимающего маршрутизатора для каждого сетевого пакета на основе его состава и секретного авторизационного ключа, известного авторизованному отправителю и принимающему маршрутизатору.

Алгоритм динамической смены *IP*-адресов по своему принципу аналогичен применяемому в радиотехнических системах алгоритму смены частоты передачи сигнала (*Frequency Hopping*): приемник и передатчик в течение интервала передачи одного сообщения синхронно переходят с одной частоты на другую, обеспечивая невозможность перехвата информации. Передатчик злоумышленника, пытающийся поставить помеху приемнику или прослушать канал связи, не знает расписания смены частот, вследствие чего не может нанести значительный ущерб работе защищенной радиолинии.

В используемом принципе роль частоты играет *IP*-адрес, изменение которого происходит в процессе передачи данных между клиентом и узлом распределенной электрической сети или интеллектуальным регулятором синхронно и по расписанию, уникальному для каждой сессии. При этом расписание, привязанное к сессии, известно только защищаемой стороне и авторизованному клиенту и является секретным для внешних наблюдателей.

Разрабатываемый метод защиты использует стек протоколов *TCP*/*IP*, а сам процесс динамической смены адресов является прозрачным как для высокоуровневых сервисов клиента, так и для самого защищаемого сервиса.

Структура и алгоритм работы защищающего кластера. В рамках предлагаемого алгоритма защиты распределительных электрических сетей сложной конфигурации от *DDoS*-атак реализуется принцип изоляции защищаемых узлов и интеллектуальных регуляторов с использованием набора управляемых высокопроизводительных фильтрующих маршрутизаторов, задачей которых является отделение легитимного трафика от атакующего. При этом отправители не знают внутреннего *IP*-адреса защищаемого узла, а обращение к нему осуществляется только через набор управляемых маршрутизаторов, формирующих защищающий кластер (рис. 1).

Структура фильтрующей сети имеет вид коллектива связанных между собой программно-конфигурируемых фильтрующих маршрутизаторов (рис. 2), осуществляющих разделение пользовательского трафика. Каждый фильтрующий маршрутизатор имеет сетевой интерфейс с *IP*-адресом, на который возможен прием пользовательских сетевых пакетов. Процесс передачи каждого сетевого пакета от пользовательского компьютера к защищаемому сервису осуществляется по маршруту (разрешенный маршрут), проходящему через строго определенный интерфейс фильтрующей сети. Разрешенный маршрут и *IP*-адрес принимающего маршрутизатора рассчитываются для каждого сетевого пакета в отдельности на основании пользовательского сертификата сессии. При этом делается предположение, что все сетевые пакеты, которые проходят по разрешенным для них маршрутам, считаются легитимными и передаются защищаемому сервису, в то время как пакеты, идущие по неразрешенным маршрутам, удаляются. Генерация расписания смены адресов осуществляется на основе данных авторизационного сертификата, который выдается контроллером защищенных

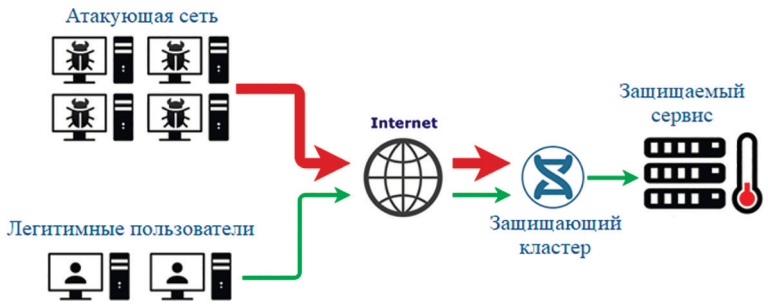

Рис. 1. Размещение защищающего кластера в сетевой инфраструктуре

Fig. 1. Placement of the protecting cluster in the network infrastructure

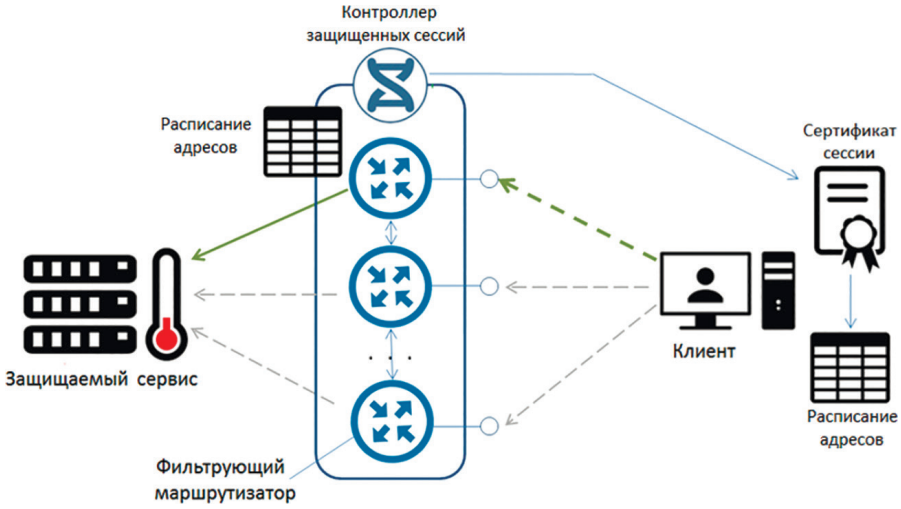

Рис. 2. Структурная схема защищающего кластера

Fig. 2. Structural diagram of the protecting cluster

сессий, входящих в защищающий кластер. Сертификат формируется контроллером для каждой сетевой сессии после прохождения клиентом процедуры авторизации.

В качестве алгоритма генерации расписания используется хеш-функция на основе необратимого алгоритма генерации псевдослучайной последовательности, представляющей собой модификацию алгоритма Фейгенбаума:

$$F(n, m, t_n) = (nF(n, m, t_0) + F(n, m, t_{t-1}))\mathrm{mod}(m),$$

где n и m – инициализационные параметры для алгоритма, которые передаются в ответном авторизационном пакете; t – номер отсчета генерируемой последовательности.

Данный алгоритм обладает равномерным распределением, что обеспечит равновероятностный выбор адресов из пула и балансировку нагрузки между маршрутизаторами.

За авторизацию клиента отвечает контроллер защищенных сессий, который принимает запросы от клиентов, формирует и передает сертификаты доступа и содержит данные обо всех сессиях. После открытия сессии контроллер передает каждому маршрутизатору значение инициальных параметров для алгоритма генерации и *IP*-адрес отправителя. После этого каждый маршрутизатор, входящий в защищающий кластер, может фильтровать пакеты, приходящие от отправителей, самостоятельно.

После прохождения авторизации отправитель осуществляет передачу данных на защищенный узел распределительной электрической сети или интеллектуальный регулятор. Формируя сетевые пакеты, отправитель заполняет поля, отвечающие за *IP*-адреса отправителя и получателя. В качестве адреса отправителя он использует свой действительный *IP*-адрес, который на протяжении всей сессии остается постоянным. *IP*-адрес назначения для каждого отправляемого пакета формируется в соответствии с полученными инициальными параметрами по алгоритму:

$$IP_{dest} = A(F(n, m, t_{cur})),$$

где t_{cur} – порядковый номер текущего пакета; $F(n, m, t)$ – алгоритм генерации псевдослучайной последовательности; $A(k)$ – функция отображения числового множества в множество *IP*-адресов пула.

После этого сформированный пакет отправляется защищающему кластеру. При получении сетевого пакета, фильтрующий маршрутизатор, используя описанный выше алгоритм генерации и данные отправителя, вычисляет адрес назначения IP_{et}. Если рассчитанный IP_{et} совпадает с адресом назначения IP_{dest} принятого пакета, то этот пакет перенаправляется на реальный адрес защищаемого узла распределенной электрической сети или интеллектуального регулятора. В противном случае этот пакет удаляется.

К предлагаемому способу защиты от *DDoS*-атак предъявляется требование: проектируемая архитектура защищающего кластера должна быть применима на практике в рамках существующей архитектуры сети Интернет. Это значит, что развертывание этой системы не должно требовать существенных изменений конфигурации и оборудования пользовательских сетей или сетей провайдеров Интернета.

Практическая реализация и результаты работы защищающего кластера. Для апробации принципа динамической смены *IP*-адреса был разработан экспериментальный образец на основе программно-конфигурируемой сети (рис. 3), способный осуществлять фильтрацию трафика. Фильтрующие маршрутизаторы реализованы в виде низкоуровневого программного обеспечения под ОС *Linux*.

В качестве эмулятора *DDoS*-атак использовался генератор трафика на основе централизованно управ-

Рис. 3. Экспериментальный образец защищающего кластера

Fig. 3. An experimental prototype of a protective cluster

ляемой клиентской сети (рис. 4), состоящей из 20 микрокомпьютеров *Cubieboard* 2 [18], с генерационной мощностью нелегитимного трафика 2 млн пакетов в секунду (2*MPPS*).

Сетевой коммутатор выступает в роли эмулятора сетевого пространства.

После сборки экспериментального стенда для подтверждения его технических характеристик проведено нагрузочное и поведенческое тестирование работы сети при различных стратегиях атак и различном соотношении числа атакующих и легальных пользователей. Для этого была разработана программа экспериментальных исследований и проведены испытания, которые подтвердили выполнение технических требований к работе стенда – сегмент генерации *DDoS*-атаки обеспечил интенсивность распределенного программно-аппаратного генератора сетевого трафика свыше 2 *MPPS*.

Программа проведения экспериментальных исследований и испытаний включает три этапа. На первом этапе проводится тестирование системы в штатном режиме без дополнительных внешних воздействий с

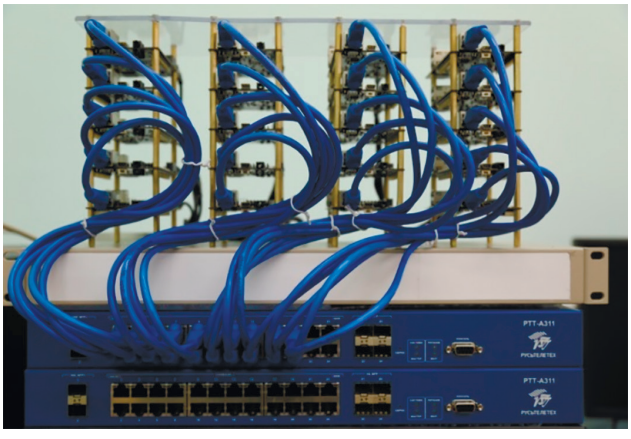

Рис. 4. Эмулятор *DDoS*-атак на базе *Cubieboard*2

Fig. 4. *DDoS*-attack emulator based on *Cubieboard*2

целью подтверждения стабильной работоспособности системы. На втором этапе с помощью эмулятора *DDoS*-атаки к легитимному трафику подмешивается нелегитимный. При этом объем нелегитимного трафика постепенно увеличивается, приводя электрическую сеть в неработоспособное состояние. На третьем этапе применяется фильтрация трафика, в результате которой энергетическая система возвращается в стабильное работоспособное состояние за счет снижения эффективности проводимой атаки.

В качестве программно-аппаратных средств, используемых для сбора данных о характеристиках работы сети при *DDoS*-атаке, использовались:

встроенные в коммутаторы аппаратные модули измерения объема проходящего трафика;

программно-аппаратный комплекс маркировки трафика;

программные анализаторы сетевого трафика.

Встроенные в аппаратные коммутаторы модули учета объема трафика представляют собой аппаратные счетчики, задачей которых являются регистрация проходящего сетевого трафика, счет пакетов и ведение статистики по интенсивности использования протоколов. Собранные статистические данные передаются по протоколу *sFlow* на компьютер, где они отображаются в виде графиков и диаграмм специализированной утилитой (*Flowalyzer NetFlo*, *sFlow Communicator*). Точность данных аппаратных счетчиков гарантируется производителем коммутатора.

Аппаратные счетчики коммутаторов используются для получения данных о суммарном объеме трафика, проходящего через сеть, и регистрации интенсивности *DDoS*-атак, имитируемых генератором трафика, построенного на основе микрокомпьютеров *Cubieboard*.

Программно-аппаратный комплекс маркировки трафика состоит:

из программных генераторов сетевых пакетов;

программных регистраторов сетевых пакетов;

сервера единого времени.

Программные генераторы легитимных пакетов служат для генерации маркированных сетевых пакетов, которые должны корректно проходить верификацию в сеть и доходить до защищаемого сервера. Каждый такой пакет несет в себе временную метку отправки, которую он получает от сервера единого времени, и счетчик, представляющий собой порядковый номер пакета в цепочке отправления. Данный пакет после прохождения защищающего кластера попадает на сервер, где в качестве сервиса используется регистратор сетевых пакетов. Последний считает приходящие пакеты, сравнивает их порядковые номера, находит разрывы в цепочках отправки пакетов и сравнивает время прихода пакета с временем его отправки.

Сервер единого времени находится в единой подсети с генераторами и регистраторами трафика и предоставляет им сервис синхронизации времени. Ввиду

непосредственно близкого расположения сервера единого времени с генераторами и регистраторами погрешность временной задержки не превышает 0,15 мкс и определяется штатными средствами сервера единого времени.

На выходе данный комплекс предоставляет следующие статистические данные:

вероятность потери пакетов в участке сети;

пропускную способность участка сети;

время прохождения пакетов участка сети.

Программно-аппаратный комплекс маркировки трафика используется для определения параметров работы сети, касающихся обслуживания легитимных пользователей, в ходе атаки.

Программные анализаторы сетевого трафика – это средства перехвата трафика, которые позволяют получать как информацию о структуре и содержимом отдельных пакетов, так и сетевого потока целиком в разрезе отдельных протоколов. В качестве основного инструмента перехвата и анализа сетевого трафика используется *Wireshark*.

Испытания проводились следующим образом. На первом этапе тестировался барьерный коммутатор: к легитимному трафику постепенно подмешивался паразитный трафик без применения разработанной технологии защиты от *DDoS*-атаки. В ходе испытаний была построена зависимость количества потерянных сетевых пакетов от проходящего через барьерный коммутатор объема трафика (рис. 5).

На основе полученных данных можно сделать вывод, что граница пропускной способности барьерного коммутатора без применения разработанной технологии защиты от *DDoS*-атаки расположена в районе 1,45 *MPPS*.

На втором этапе испытаний в работу вступает защищающий кластер. По данным испытаний построен график изменения количества потерянных пакетов при устоявшейся атаке объемом 2,4 *MPPS* (рис. 6).

Из графика (рис. 6) видно, что потери сетевых пакетов составляют 0,98–1,15 %, что компенсируется сервисами транспортного уровня путем повторной отправки сетевых пакетов [19]. При этом 92 % нелегитимного трафика было отфильтровано.

Основываясь на аддитивности пропускной способности барьерных коммутаторов, можно сказать, что для разработанного защищаемого кластера пропускная способность будет ограничиваться серверами верификации и достигает 4,35 *MPPS*.

Выводы. Необходимость эффективного использования энергии обусловливает масштабное внедрение цифровых технологий, превращая энергетическую индустрию в интеллектуальную оптимизированную систему поставки электроэнергии. При этом растет роль средств защиты информационной безопасности распределительных электрических сетей, в частности от *DDoS*-атак. В ходе исследования решены следующие технические задачи: разработана модель, имитирующая атаку *DDoS* на информационный кластер электрической сети; разработана модель защищающего кластера, устраняющего атаку *DDoS* электрической сети; разработаны экспериментальные образцы эмулятора *DDoS*-атак и защищающего кластера для фильтрации трафика.

Проведено моделирование работы информационного кластера электрической сети в следующих условиях:

в штатном режиме без кибератаки *DDoS* – система работает стабильно;

при наличии атаки *DDoS* от эмулятора без проведения фильтрации трафика – информационный кластер электрической сети перешел в неработоспособное состояние;

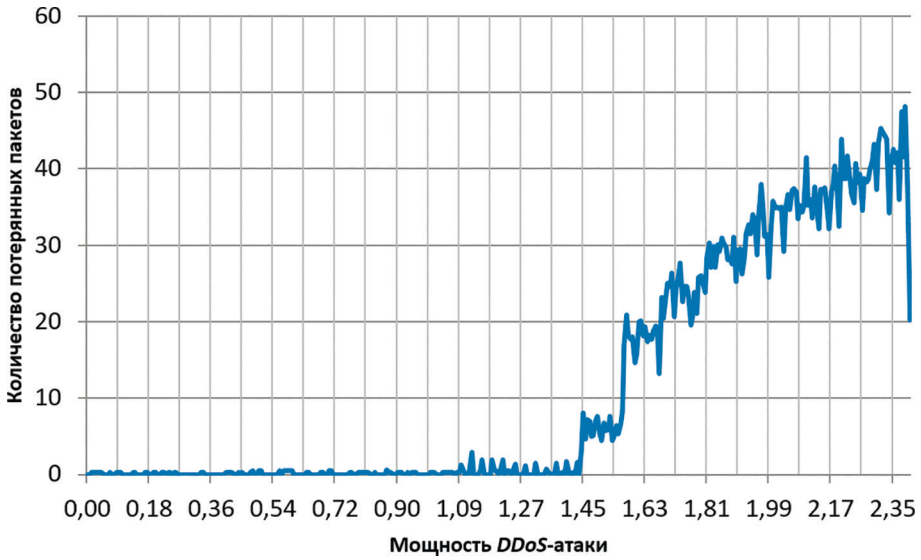

Рис. 5. Зависимость количества потерянных сетевых пакетов от мощности *DDoS*-атаки

Fig. 5. The dependence of the number of lost network packets on the power of a DDoS attack

Рис. 6. Потери сетевого пакета при веерной атаке в 2,4 *MPPS*, %

Fig. 6. Network packet loss in a fan attack of 2.4 MPPS, %

при наличии атаки *DDoS* от эмулятора с проведением фильтрации трафика – эффективность атаки значительно снизилась, вероятность потери легитимных пакетов в пределах допуска.

Проведенные исследования экспериментального образца показали, что разработанная технология на основе несемантической фильтрации сетевого трафика позволяет противодействовать распределенным *DDoS*-атакам, снижая интенсивность атак не менее чем на 92 % при вероятности потери пакетов менее 2 %, а также попыткам несанкционированного доступа к трафику между клиентом и узлом распределительной электрической сети или интеллектуальным регулятором, что говорит об эффективности разработанного метода противодействия *DDoS*-атакам на информационные кластеры энергетических систем.

Исследование выполнено за счет гранта РНФ (проект № 20-19-00541).

СПИСОК ЛИТЕРАТУРЫ

1. **Tan Y.S., Ng Y.T., Low J.S.C.** Internet-of-Things Enabled Real-Time Monitoring of Energy Efficiency on Manufacturing Shop Floors. Procedia CIRP, 2017, 61, 376–381, DOI:10.1016/j.procir.2016.11.242.

2. **Бутырин П.А., Алпатов М.Е.** Цифровизация и аналитика в электротехнике. Цифровые двойники трансформаторов. – Электричество, 2021, № 10, с. 4–10.

3. **Воропай Н.И.** От плана ГОЭЛРО к глобальному электроэнергетическому интернету. – Электричество, 2020, № 12, с. 10–13.

4. **Колосок И.Н., Гурина Л.А.** Идентификация кибератак на системы *SCADA* и СМПР в ЭЭС при обработке измерений методами оценивания состояния. – Электричество, 2021, № 6, с. 25–32.

5. **Взлом** и проникновение. Энергетики и госструктуры взялись за кибербезопасность [Электрон. ресурс], URL: https://www.kommersant.ru/doc/4198110 (дата обращения 29.05.2021).

6. **Что такое DDoS-атака** [Электрон/ ресурс], URL: https://qrator.net/ru/solutions/ddos/how-qrator-works#s27 (дата обращения 29.05.2021).

7. **Массель А.Г., Гаськова Д.А.** Методы и подходы к обеспечению кибербезопасности объектов цифровой энергетики. – Энергетическая политика, 2018, № 5, с. 62–72.

8. **Chakhchoukh Y., Ishii H.** Cyber-Attacks Scenarios on the Measurement Function of Power State Estimation. – American Control Conference (ACC), Chicago, IL, USA, 2015, pp. 3676–3681.

9. **Chakhchoukh Y., Ishii H.** Enhancing Robustness to CyberAttacks in Power Systems Through Multiple Least Trimmed Squares State Estimations. – IEEE Transactions on Power Systems, 2016, vol. 31 (6), pp. 4395–4405.

10. **Zhuang P., Deng R., Liang H.** False Data Injection Attacks Against State Estimation in Multiphase and Unbalanced Smart Distribution Systems. – IEEE Transactions on Smart Grid, 2019, vol. 10 (6), pp. 6000–6013.

11. **Хохлов М.В.** Уязвимость оценивания состояния ЭЭС к кибератакам. – Материалы международ. научного семинара им. Ю.Н. Руденко «Методические вопросы исследования надежности больших систем энергетики», 2015, с. 557–566.

12. **Ежегодный** отчет Qrator Labs о сетевой безопасности и доступности [Электрон. ресурс], URL: https://blog.qrator.net/ru/2019-report-ru_64 (дата обращения 29.05.2021).

13. **В «Ростелеком-Солар»** прошли киберучения по защищённости объектов электроэнергетики [Электрон. ресурс], URL: https://rt-solar.ru/events/news/1758 (дата обращения 29.05.2021).

14. **Song T., et al.** A Privacy Preserving Communication Protocol for IoT Applications in Smart Homes. – IEEE Internet Things J., 2017, No. 4, pp. 1844–1852.

15. **Roman R., Lopez J.** Security in the Distributed Internet of Things. – 2012 International Conference on Trusted Systems, London, UK, 2012, pp. 65–66.

16. **Sosnina E., et al.** Voltage Control with Thyristor-Regulated Booster Transformer. – 2018 International Conference on Smart Grid (icSmartGrid), 2018, pp. 202–207, DOI:10.1109/ISGWCP.2018.8634477.

17. **Krylov V.V., Kravtsov K.N.** DDoS Attack and Interception Resistance IP Fast Hopping Based Protocol. – ArXive, Cornell University, 2012.

18. **Микрокомпьютер** Raspberry Pi Model B+ [Электрон. ресурс], URL: http://www.dns-shop.ru/product/6bf2486e24083120/mikrokomputer-raspberry-pi-model-b/ (дата обращения 29.05.2021).

19. **TCP/IP** [Электрон. ресурс], URL: https://ru.wikipedia.org/wiki/TCP/IPel-b/ (дата обращения 01.09.2021).

[03.09.2021]

Авторы: ***Дмитриев Дмитрий Валерьевич*** *– кандидат техн. наук, доцент кафедры «Информатика и системы управления» Нижегородского государственного технического университета им. Р.Е. Алексеева, Н.Новгород, Россия.*

Ляхманов Дмитрий Александрович *– кандидат техн. наук, доцент кафедры «Информатика и системы управления» Нижегородского государственного технического университета им. Р.Е. Алексеева, Н.Новгород, Россия.*

Соколова Элеонора Станиславовна *– доктор техн. наук, профессор кафедры «Информатика и системы управления» Нижегородского государственного технического университета им. Р.Е. Алексеева, Н.Новгород, Россия.*

Elektrichestvo, 2022, No. 3, pp. 49–57 ***DOI:10.24160/0013-5380-2022-3-49-57***

Combating DDoS Cyberattacks in the Energy Sector

DMITRIEV Dmitriy V. *(Nizhny Novgorod State Technical University n.a. R.E. Alekseev, Nizhny Novgorod, Russia) – Docent of the Informatics and Control Systems Dept, Cand. Sci. (Eng.).*

LYAKHMANOV Dmitriy A. *(Nizhny Novgorod State Technical University n.a. R.E. Alekseev, Nizhny Novgorod, Russia) – Docent of the Informatics and Control Systems Dept., Cand. Sci. (Eng.).*

SOKOLOVA Eleonora S. *(Nizhny Novgorod State Technical University n.a. R.E. Alekseev, Nizhny Novgorod, Russia) – Professor of the the Informatics and Control Systems Dept, Dr. Sci. (Eng.).*

Digitalization of infrastructures with the use of information technologies for efficient intelligent management of power systems and their having rather poor cybersecurity are factors provoking a growing number of cyberattacks in the energy sector. At the same time, the energy sector structural units are critically important facilities malfunctioning of which compromises the national security. The problem has become so serious that cyberattacks on the energy sector infrastructural facilities are seen by the governments of many states as real threats leading to malfunctioning of the fuel and energy complex facilities. There is a steady growth of distributed denial-of-service (DDoS) attacks targeted on energy sector facilities. Electric energy building and control automation systems and call centers of power generating companies are attacked, causing power supply to entire regions become upset for a long period of time. At present, there are no reliable and universal technologies capable to block DDoS attacks. The article describes a method for combating DDoS attacks in power systems based on non-semantic filtering of traffic. The article also presents a new approach to combating DDoS attacks, which protects servers and traffic bandwidth. The proposed approach is based on the interaction of users with server equipment by dynamically changing the IP addresses of the attacked resources according to a pseudo-randomly generated schedule. The developed technology for filtering the network traffic makes it possible to combat DDoS attacks, reducing their intensity by about 92 %. As a result, the loss of legitimate packets, which is unavoidable in implementing any DDoS combating technology, makes less than 2 %.

K e y w o r d s: *smart energy, energy sector digitalization, distributed attacks, cybersecurity*

The study was carried out at the expense of the RGNF grant (Project No. 20-19-00541).

REFERENCES

1. **Tan Y.S., Ng Y.T., Low J.S.C.** Internet-of-Things Enabled Real-Time Monitoring of Energy Efficiency on Manufacturing Shop Floors. Procedia CIRP, 2017, 61, 376–381, DOI:10.1016/j.procir.2016.11.242.

2. **Butyrin P.A., Alpatov M.E.** *Elektrichestvo – in Russ. (Electricity)*, 2021, No. 10, pp. 4–10.

3. **Voropay N.I.** *Elektrichestvo – in Russ. (Electricity)*, 2020, No. 12, pp. 10–13.

4. **Kolosok I.N., Gurina L.A.** *Elektrichestvo – in Russ. (Electricity)*, 2021, No. 6, pp. 25–32.

5. ***Vzlom*** *i proniknovenie. Energetiki i gosstruktury vzyalis' za kiberbezopasnost'* (Breaking and Entering. Energy and Government Agencies Have Taken up Cybersecurity) [Electron. resource], URL: https://www.kommersant.ru/doc/4198110 (Date of appeal 29.05.2021).

6. ***Chto takoe DDoS-ataka*** (What is a DDoS Attack) [Electron. resource], URL: https://qrator.net/ru/solutions/ddos/how-qrator-works#s27 (Date of appeal 29.05.2021).

7. **Massel A.G., Gas'kova D.A.** *Energeticheskaya politika – in Russ. (Energy Policy)*, 2018, No. 5, pp. 62–72.

8. **Chakhchoukh Y., Ishii H.** Cyber-Attacks Scenarios on the Measurement Function of Power State Estimation. – American Control Conference (ACC), Chicago, IL, USA, 2015, pp. 3676–3681.

9. **Chakhchoukh Y., Ishii H.** Enhancing Robustness to CyberAttacks in Power Systems Through Multiple Least Trimmed Squares State Estimations. – IEEE Transactions on Power Systems, 2016, vol. 31 (6), pp. 4395–4405.

10. **Zhuang P., Deng R., Liang H.** False Data Injection Attacks Against State Estimation in Multiphase and Unbalanced Smart Distribution Systems. – IEEE Transactions on Smart Grid, 2019, vol. 10 (6), pp. 6000–6013.

11. **Khokhlov M.V.** *Materialy mezhdunarod. nauchnogo seminara im. Yu.N. Rudenko «Metodicheskie voprosy issledovaniya nadezhnosti bol'shikh sistem energetiki» – in Russ. (Materials of the International Scientific Seminar n. a. Yu.N. Rudenko "Methodological*

Issues of Reliability Research of Large Power Systems"), 2015, pp. 557–566.

12. ***Ezhegodnyy** otchet Qrator Labs o setevoy bezopasnosti i dostupnosti* (QratorLabs Annual Report on Network Security and Availability) [Electron. resource], URL: https://blog.qrator.net/ru/2019-report-ru_64 (Date of appeal 29.05.2021).

13. ***V «Rostelekom-Solar»** proshli kiberucheniya po zashchishchyonnosti ob"ektov elektroenergetiki* (At Rostelecom-Solar, Cyber-Trainings on the Security of Electric Power Facilities Were Held) [Electron. resource], URL: https://rt-solar.ru/events/news/1758 (Date of appeal 29.05.2021).

14. **Song T., et al.** A Privacy Preserving Communication Protocol for IoT Applications in Smart Homes. – IEEE Internet Things J., 2017, No. 4, pp. 1844–1852.

15. **Roman R., Lopez J.** Security in the Distributed Internet of Things. – 2012 International Conference on Trusted Systems, London, UK, 2012, pp. 65–66.

16. **Sosnina E., et al.** Voltage Control with Thyristor-Regulated Booster Transformer. – 2018 International Conference on Smart Grid (icSmartGrid), 2018, pp. 202–207, DOI:10.1109/ISGWCP.2018.8634477.

17. **Krylov V.V., Kravtsov K.N.** DDoS Attack and Interception Resistance IP Fast Hopping Based Protocol. – ArXive, Cornell University, 2012.

18. **Microcomputer** Raspberry Pi Model B+ [Electron. resource], URL: http://www.dns-shop.ru/product/6bf2486e24083120/mikrokomputer-raspberry-pi-model-b/ (Date of appeal 29.05.2021).

19. **TCP/IP** [Electron. resource], URL: https://ru.wikipedia.org/wiki/TCP/IPel-b/ (Date of appeal 01.09.2021).

[03.09.2021]