05.14.02 Электростанции и электроэнергетические системы

УДК 621.391

**Стребкова Татьяна Владимировна, Тучина Дарья Сергеевна,
Звада Павел Александрович**

ПРОВЕДЕНИЕ ПРАКТИЧЕСКОЙ КИБЕРАТАКИ НА КАНАЛ ПЕРЕДАЧИ ДАННЫХ ЦИФРОВОЙ ПОДСТАНЦИИ

Развитие информационных систем в электроэнергетическом комплексе повлекло за собой появление проблем обеспечения кибербезопасности. Чтобы оценить влияние, оказываемое различными видами кибератак на стабильность функционирования цифровой подстанции, в данной работе описаны две произведенные экспериментальные атаки на смоделированный канал передачи данных. Показаны особенности функционирования электрических подстанций нового поколения, технологии тестирования электрических подстанций современным программным продуктом EDScout от OMICRON, позволяющим не только оценивать потоки данных от технологических устройств, но и эмитировать их. На основе анализа полученных результатов предложены решения обозначенной проблемы, направленные на поддержку устройствами функций проверки содержимого сообщений GOOSE.

Ключевые слова: *кибербезопасность, цифровые подстанции, МЭК 61850, спуфинг, DDoS-атака.*

Tatiana Strebkova, Darya Tuchina, Pavel Zvada

THE PRACTICAL CYBERATTACK ON THE DATA TRANSMISSION CHANNEL OF THE DIGITAL SUBSTATION

The development of information systems in the electric power complex has led to the emergence of problems ensuring cyber security. In order to assess the impact of different types of cyber-attacks on the stability of the digital substation, in this work two experimental attacks were made on the simulated data transmission channel. The features of the operation of electrical substations of the new generation, the technology of testing electrical substations with modern software product EDScout from OMICRON, allowing not only to evaluate data streams from technological devices, but also to emit them are shown. Based on the analysis of the results obtained, solutions to the indicated problem were proposed, with devices supporting the functions of checking the content of GOOSE messages.

Key words: *cybersecurity, digital substations, IEC 61850, spoofing, DDoS attack.*

Введение / Introduction. Ни для кого не секрет, что за последнее десятилетие в электроэнергетике процессы автоматизации и цифровизации ускорились в несколько раз. Произошло множество принципиальных изменений в структуре построения подстанций. Появились новые протоколы и стандарты, описывающие каждый протекающий процесс на теперь уже цифровой подстанции [7, 8]. Однако вместе с инновациями открылись и новые проблемы, одной из которых является обеспечение кибербезопасности передачи данных, интеллектуальных электронных устройств (ИЭУ), серверов и энергообъектов в целом. Объем потенциальных мест атаки зависит в целом от применяемых топологий цифровых подстанций, то есть от объема и типов цифрового оборудования электрической подстанции. Можно обозначить несколько уровней потенциальных вторжений: уровень шины процесса, шины станции, системы синхронизации устройств подстанции.

Последствия кибератак на данный момент трудно переоценить – от выхода из строя одного элемента подстанции до гибели людей [1]. Они могут непосредственно повлиять на стабильность и надежность энергосистемы. Так как архитектура обмена данными на цифровой подстанции имеет довольно сложную структуру, то оценка влияния кибератак на разных её уровнях требует детального изучения ввиду неоднозначности оценки последствий. Так, например, атака на цифровой терминал релейной защиты может привести как к ложному отключению одного из круп-

ных потребителей, так и к ложному срабатыванию одной из систем автоматики, и к отключению системных связей. Чтобы исследовать это влияние в данной работе будет описано осуществление практической атаки на канал передачи данных между ИЭУ и управляемым оборудованием (выключателем) [4].

В данной работе будут продемонстрированы две наиболее опасные атаки: подмена данных или устройства управления (спуфинг), DDoS-атака [3].

Материалы и методы / Materials and methods. Приведенная ниже атака была реализована в качестве демонстрации уязвимости канала передачи данных по протоколу GOOSE, созданного на базе лабораторного комплекса СКФУ.

Данный канал связи имитирует шину процесса подстанции, которая соединяет ИЭУ и выключатель. Программа, написанная с помощью среды графического моделирования LabView, состоит из двух частей (рис. 1):

1 – устройство-отправитель информации – генерация GOOSE-сообщений;

2 – устройство-получатель информации – выборочный прием сообщений, в зависимости от настроек подписки, на перечень устройств от которых разрешен прием сообщений.

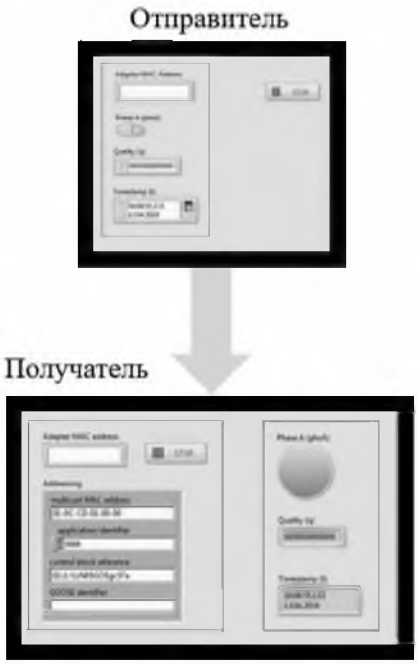

Рис. 1. Схема устройств отправителей и получателей при посылке GOOSE-сообщений по стандарту МЭК 61850

Для обеспечения достоверности эксперимента перед проведением исследований созданный канал передачи данных был подвержен проверке функциональности и соответствию стандарту МЭК 61850 – скорость информационного обмена не превысила нормируемых значений задержки передаваемых сообщений.

Цель создания шины процесса – проведение комплексной проверки устойчивой работы канала передачи данных, при возникновении угрозы извне – проведения кибератак.

При проведении эксперимента со спуфинг-атакой мы условно разделяем устройства-отправители информации на «истинные» и «ложные». Описанная выше имитируемая шина процесса является истинной в эксперименте. Истинное ИЭУ отправляет сигналы false (команда несрабаты-

вания) на выключатель. Ложным (атакующим) устройством является ИЭУ, созданное на базе ПК EDScout. Оно отправляет сигналы, противоположные сигналам истинного устройства true (команда на срабатывание). Таким образом, мы можем наблюдать, как устройство-получатель распознает приходящие пакеты информации и может ли оно отличить истинный сигнал от ложного (рис. 2).

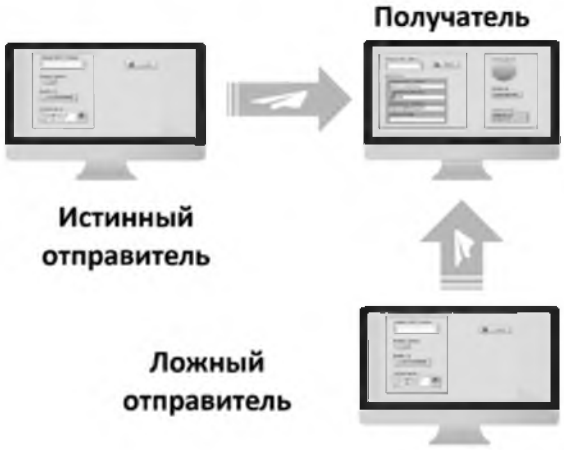

Рис. 2. Схема эксперимента спуфинг-атаки

Второй эксперимент проводится с использованием того же канала передачи GOOSE-сообщений. На него с помощью программы Scapy посылается множество генерируемых запросов с целью затормозить или вовсе остановить процесс передачи истинных пакетов (рис. 3).

В данном эксперименте используются 3 компьютера в качестве атакующих устройств, с которых отправляются ложные запросы, требующие дополнительной обработки устройством-получателем.

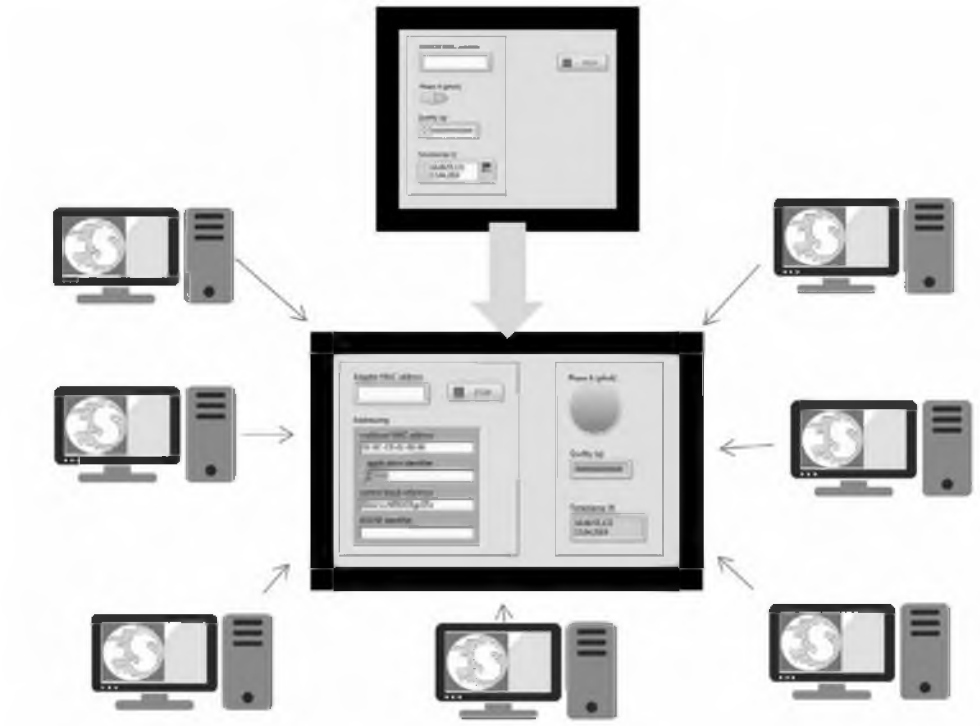

Рис. 3. Схема эксперимента DDoS-атаки

Результаты и обсуждение / Results and discussion. В случае спуфинг-атаки результат оценивался с помощью программы Wireshark, которая предназначена для отслеживания, регистрации и мониторинга трафика в сети. Из рис. 4 видно, что получатель передаваемых сигналов не распознал ложные пакеты и не отфильтровал их. Также метка качества не изменилась и указана «good» [5], то есть данные воспринимаются как достоверные. Хотя это вовсе не так.

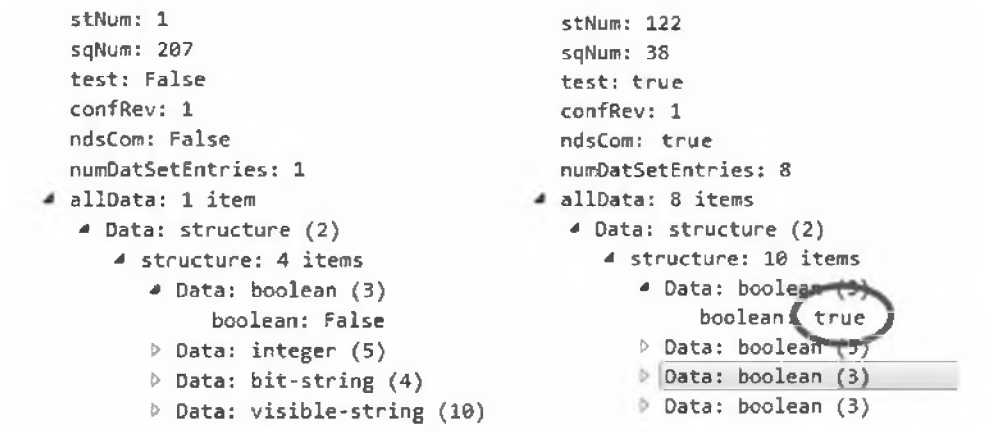

Рис. 4. Передаваемый пакет с истинного устройства (слева) и с ложного (справа)

Во время проведения эксперимента с DDoS-атакой результаты анализировались с помощью Диспетчера задач Windows. Мы наблюдали изменение загрузки локальной сети от количества устройств посылающих запросы.

В нормальном состоянии информационная сеть не загружена, что беспрепятственно позволяет осуществлять обмен GOOSE-сообщениями. Далее, извне было произведено подключение нескольких несанкционированных пользователей, выполняющих роль генераторов ложных сообщений. В результате их присоединения может возникнуть режим повышенной информационной нагрузки, что, в свою очередь, поставит под угрозу вопрос целостности передаваемых данных и возможности возникновения временных задержек GOOSE-коммуникации.

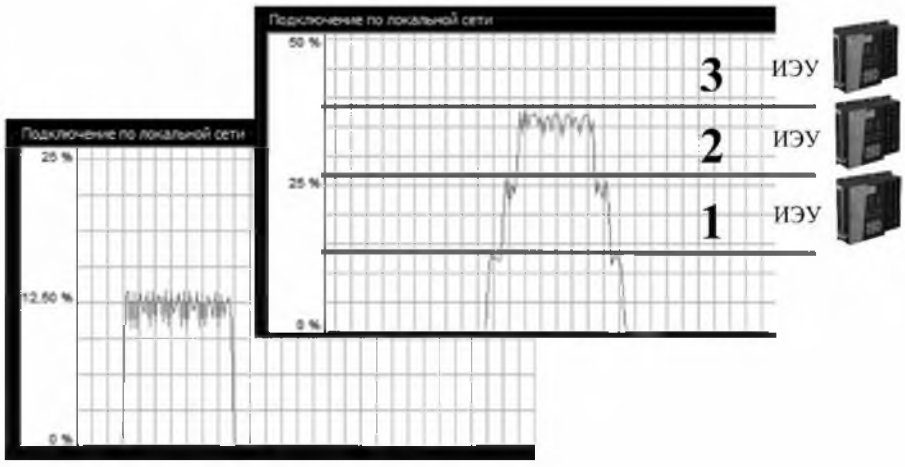

Рис. 5. Степень загрузки сети от количества подключающихся атакующих устройств

В процессе эксплуатации созданной шины процесса была проведена экспериментальная DDoS-атака с помощью включения в сеть 3 компьютеров. Их постоянно генерирующиеся запросы были направленны на самый загруженный элемент сети – устройство приемник, тем самым

увеличив загрузку информационного канала до 37 % (рис. 5). В случае проведения полноценной DDoS-атаки с участием тысячи таких компьютеров (ботнета – совокупности устройств, используемых злоумышленником для совершения DDoS-атак) возникнет перегрузка информационной сети и образование временных задержек при передаче сообщений. Следует отметить, что при передаче GOOSE-сообщений задержки в канале связи являются критическими, так как это впоследствии может привести к отказу коммуникационного оборудования.

Заключение / Conclusion. Мы продемонстрировали, что простая атака позволяет вредоносным программам контролировать оборудование управления с поддержкой МЭК 61850. Несмотря на отсутствие четкого определения того, как обеспечить безопасность передачи сообщений GOOSE, энергетические компании должны принять не только физические, но и кибермеры для предотвращения такого рода атак.

Для предотвращения инсайдерских атак необходимо, чтобы на конечных устройствах были реализованы алгоритмы безопасности для шифрования пакетов или добавления цифровой подписи, чтобы они не могли отслеживаться злоумышленником, проходя проверку подлинности, и чтобы поддельные пакеты не могли быть отправлены. Устаревшие ИЭУ и устройства с низкой пропускной способностью не могут поддерживать эти криптографические алгоритмы. Такое решение, как добавление внешнего модуля безопасности к сетевым интерфейсам в каждом ИЭУ, увеличивает время обработки и провоцирует дополнительные режимы отказа. Этот метод может быть добавлен только к коммутаторам и некоторому ключевому оборудованию, чтобы обеспечить их частичную защиту.

Альтернативным подходом может являться использование коммутаторов и маршрутизаторов, которые поддерживают протокол МЭК 61850 и проверяют содержимое сообщения GOOSE. При таком подходе сеть сможет сбрасывать или генерировать аварийные сигналы в случае обнаружения логически несовместимых сообщений (например, пакеты с одинаковым MAC-адресом, поступающие из разных портов коммутатора, или сообщения, не соответствующие конфигурации МЭК 61850, как в случае с DDoS-атакой).

Также на сегодняшний день в структуре подстанций предусмотрена одноуровневая система защиты Firewall, которая устанавливается на верхнем (подстанционном) уровне [2; 9]. Мы предлагаем трехуровневую систему Firewall, чтобы каждый уровень подстанции был максимально защищен от различного рода атак.

ЛИТЕРАТУРА И ИНТЕРНЕТ-РЕСУРСЫ

1. Information analysis and infrastructure protection / Department of Homeland Security. Critical Infrastructure Information Act of 2002 [Online]. URL: http://www.dhs.gov/xlibrary/assets/CII_Act.pdf
2. Общие принципы достоверизации ТМ в ОИК ОДУ Урала и РДУ ОЭС Урала // Приложение 1 к письму ОДУ Урала от 13.07.2015 № 060-в-V-19-3795
3. Георгица И. В., Гончаров С. А., Мохов В. А. Мультиагентное моделирование сетевой атаки типа DDoS // ИВД. 2013. № 3 (26). URL: https://cyberleninka.ru/article/n/multiagentnoe-modelirovanie-setevoy-ataki-tipa-ddos (дата обращения: 20.04.2019)
4. Hoyos J., Dehus M., Brown T. X. Exploiting the GOOSE Protocol: A Practical Attack on Cyber-infrastructure // 2012 IEEE Globecom Workshops, 2012. P. 1508–1513.
5. Ковцова И. О. Обработка и передача учетных данных для классических и цифровых электроподстанций: монография. М.: Прометей, 2016. 236 с.
6. Стандарт организации ПАО «ФСК ЕЭС» СТО 56947007-29.240.10.265-2019 Общие требования к метрологическому контролю измерительных каналов ЦПС. Дата введения: 25.03.2019.
7. ГОСТ Р МЭК 61850-5-2011. Сети и системы связи на подстанциях. Часть 5. Требования к связи для функций и моделей устройств. Дата введения 2012-09-01.

8. Стандарт организации ПАО «ФСК ЕЭС» СТО 56947007-29.240.10.253-2018 Типовые методики испытаний компонентов ЦПС на соответствие стандарту МЭК 61850 первой и второй редакций. Дата введения: 29.03.2018.
9. Стандарт организации ПАО «ФСК ЕЭС» СТО 56947007-29.240.10.256-2018 Технические требования к аппаратно-программным средствам и электротехническому оборудованию ЦПС. Дата введения: 21.09.2018

REFERENCES AND INTERNET RESOURCES

1. Information analysis and infrastructure protection / Department of Homeland Security. Critical Infrastructure Information Act of 2002, [Online]. URL: http://www.dhs.gov/xlibrary/assets/CII_Act.pdf
2. Obshchie printsipy dostoverizatsii TM v OIK ODU Urala i RDU OES Urala (General principles of the TM verification in the OIK ODU of the Urals and RDU OES of the Urals) // Prilozhenie 1 k pis'mu ODU Urala ot 13.07.2015 № 060-v-V-19-3795
3. Georgitsa I. V., Goncharov S. A., Mokhov V. A. Mul'tiagentnoe modelirovanie setevoi ataki tipa DDoS (Multi-agent simulation of network attack type DDoS) // IVD. 2013. № 3 (26). URL: https://cyberleninka.ru/article/n/multiagentnoe-modelirovanie-setevoy-ataki-tipa-ddos (дата обращения: 20.04.2019)
4. Hoyos J., Dehus M., Brown T. X. Exploiting the GOOSE Protocol: A Practical Attack on Cyber-infrastructure // 2012 IEEE Globecom Workshops, 2012. P. 1508–1513.
5. Kovtsova I. O. Obrabotka i peredacha uchetnykh dannykh dlya klassicheskikh i tsifrovykh elektropodstantsii (Processing and transmission of accounting data for classic and digital power substations): monografiya. M.: Prometei, 2016. 236 s.
6. Standart organizatsii PAO «FSK EES» STO 56947007-29.240.10.265-2019 Obshchie trebovaniya k metrologicheskomu kontrolyu izmeritel'nykh kanalov TsPS (General requirements for the metrological control of measuring channels of digital substations). Data vvedeniya: 25.03.2019
7. GOST R IEC 61850-5-2011. Seti i sistemy svyazi na podstantsiyakh. Chast' 5. Trebovaniya k svyazi dlya funktsii i modelei ustroistv (Networks and communication systems at substations. Part 5. Communication requirements for features and device models). Data vvedeniya 2012-09-01.
8. Standart organizatsii PAO «FSK EES» STO 56947007-29.240.10.253-2018 Tipovye metodiki ispytanii komponentov TsPS na sootvetstvie standartu IEC 61850 pervoi i vtoroi redaktsii (Typical test procedures for components of digital substations for compliance with IEC 61850 first and second editions). Data vvedeniya: 29.03.2018.
9. Standart organizatsii PAO «FSK EES» STO 56947007-29.240.10.256-2018 Tekhnicheskie trebovaniya k apparatno-programmnym sredstvam i elektrotekhnicheskomu oborudovaniyu TsPS (Technical requirements for hardware and software and electrical equipment of digital substations). Data vvedeniya: 21.09.2018.

СВЕДЕНИЯ ОБ АВТОРАХ

Стребкова Татьяна Владимировна, магистрант 1 курса кафедры автоматизированных электроэнергетических систем и электроснабжения инженерного института Северо-Кавказского федерального университета. E-mail: tanya.strebkova@mail.ru.

Тучина Дарья Сергеевна, магистрант 2 курса кафедры автоматизированных электроэнергетических систем и электроснабжения инженерного института Северо-Кавказского федерального университета. E-mail: tuchinads@yandex.ru.

Звада Павел Александрович, старший преподаватель кафедры автоматизированных электроэнергетических систем и электроснабжения инженерного института Северо-Кавказского федерального университета. E-mail: zpass1781@mail.ru.

INFORMATION ABOUT AUTHORS

Tatiana Strebkova, 1st year undergraduate of the Department of Automated Electric Power Systems and Power Supply of the Engineering Institute of North Caucasus Federal University. E-mail: tanya.strebkova@mail.ru.

Darya Tuchina, 2nd year undergraduate of the Department of Automated Electric Power Systems and Power Supply of the Engineering Institute of North Caucasus Federal University. E-mail: tuchinads@yandex.ru.

Pavel Zvada, Senior Lecturer of the Department of Automated Electric Power Systems and Power Supply of the Engineering Institute of North Caucasus Federal University. E-mail: zpass1781@mail.ru.