УСОВЕРШЕНСТВОВАНИЕ МЕТОДИКИ ИСПЫТАНИЯ ПРОГРАММНО-ТЕХНИЧЕСКОГО КОМПЛЕКСА АСУ ТП НА БАЗЕ СТАНДАРТА МЭК 61850

АВТОРЫ:

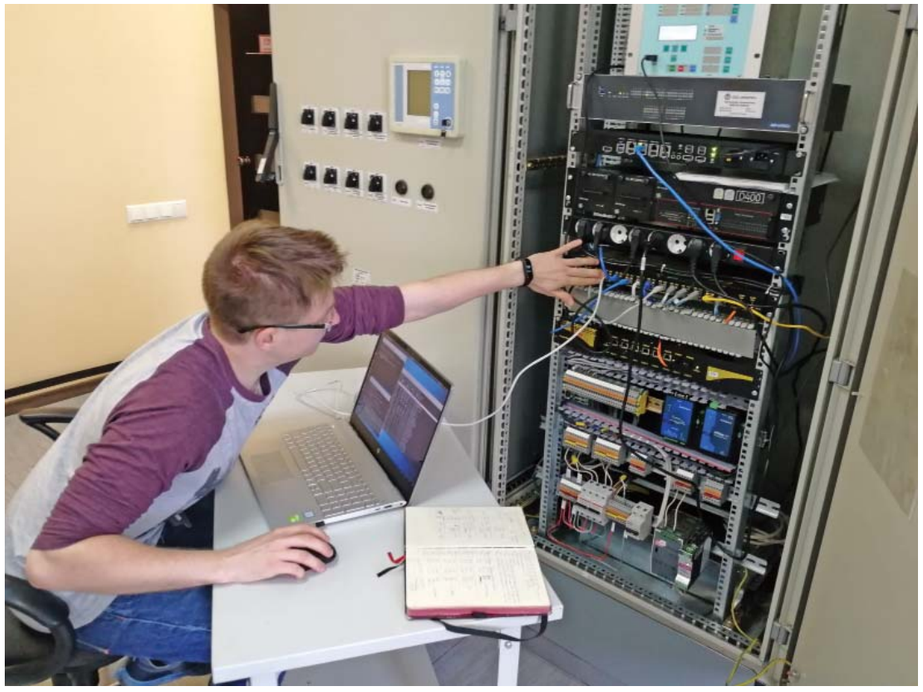
В.В. КРУГЛИКОВ,
ПАО «ФСК ЕЭС»,
ХАБАРОВСКОЕ ПМЭС

А.Г. ТКАЧЕНКО,
ПАО «ФСК ЕЭС» —
МЭС ВОСТОКА

А.М. КОНСТАНТИНОВ,
К.Т.Н.,
ДАЛЬНЕВОСТОЧНЫЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЙ

Использование цифровых технологий на подстанциях — это общемировой тренд современной электроэнергетики. Ключевой задачей применения данных инноваций является создание надежного программно-технического комплекса, благодаря которому подстанция сможет бесперебойно функционировать в информационной взаимосвязи со всем техническим оборудованием.

Ключевые слова: цифровая подстанция; МЭК; IEC; МЭК 61850; АСУ ТП; информационная безопасность; DDos; Kali Linux.



Испытания программно-технического комплекса АСУ ТП

ВВЕДЕНИЕ

В связи с быстрым развитием вычислительной техники и информационных технологий важной задачей стал поиск инновационных решений в области управления и организации электроэнергетических систем и сетей. Повсеместное использование цифровых технологий на подстанциях является инновационным методом в энергетике. Если раньше внутри подстанции между цифровыми устройствами применяли МЭК 60870-101/104, то теперь в РФ стал широко применяться МЭК 61850. Этот стандарт играет важную роль в деле внедрения технологии «Цифровая подстанция» и создании интеллектуальных сетей, поскольку позволяет создать унифицированную платформу для доступа и обмена информацией между микропроцессорным оборудованием различных производителей. Основным преимуществом систем на базе МЭК 61850 является то, что они обеспечивают более высокую скорость и безопасность передачи информации по сравнению с МЭК 60870.

Вопросы надежности программно-технического комплекса (ПТК) АСУ ТП или системы сбора и передачи информации (ССПИ) всегда имели большое значение. С каждым годом количество интеллектуальных электронных устройств (ИЭУ) растет, и, как следствие, растет объем трафика, протекающего в технологических сетях подстанции или иного объекта. Но сможет ли действующий ПТК справиться с постоянно растущим потоком данных? На данный вопрос дает ответ методика, описанная в СТО 56947007-25.040.40.112-2011 [2], которая предлагает проверку АСУ ТП и/или ССПИ в режимах «информационный шторм» и «информационный всплеск». Она применяется при аттестации оборудования, описывает методы и нормы испытаний, но не рассматривает вопрос об исследованиях нагрузочных характеристик оборудования комплекса.

Следует отметить, что СТО 56947007-25.040.40.112-2011 не применим на действующих объектах, потому что оборудование, установленное на объектах, не соответствует условиям испытаний, указанным в методике, в то же время такие испытания не могут проводиться без нарушения технологического процесса. Данный стандарт не дает четких рекомендаций для проведения испытаний на действующих объектах, так как в методике четко оговорено количество (превышающее число установленных на объектах) необходимых терминалов релейной защиты и автоматики (РЗА), коммутаторов, контроллеров и пр.

Согласно СТО 56947007-25.040.40.112-2011 [1], выбор оборудования для проведения испытаний, а также состав сигналов определяются главной схемой подстанции (ПС). В зависимости от главной схемы подстанции и моделируемой аварии информационная нагрузка на ПТК АСУ ТП может существенно различаться. Результаты проводимых испытаний должны давать возможность сопоставлять производительность комплексов АСУ ТП различных производителей. В связи с этим испытания должны проводиться при одной схеме моделируемой ПС.

При построении цифровой подстанции необходимо разработать ПТК, благодаря которому данная ПС будет функционировать в информационной взаимосвязи с оборудованием. ПТК должен разрабатываться как единая, интегрированная, иерархическая распределенная человеко-машинная система, оснащенная средствами управления, измерения, сбора, обработки, отображения, регистрации, хранения и передачи информации.

СТО 56947007-25.040.40.160-2013 [2] предлагает проверку при реконструкции и новом строительстве, но не предусматривает проверку всего ПТК в режиме лавинообразной передачи/приема информации. Это имеет значение для случаев, когда происходит масштабная авария. Так, в среднем один терминал РЗА генерирует 70 и более сигналов, причем аварийных из них — около 50. Например, на крупной ПС 220 кВ установлено около 29 терминалов. Если происходит масштабная авария, то за одну секунду может сгенерироваться свыше 2000 сигналов. Данный всплеск может довольно значительно переполнить информационный канал и таким образом стать причиной недопоставки части информации из-за информационной перегрузки как терминалов РЗА, так и всего ПТК. Это подтверждает необходимость исследования влияния информационной нагрузки на работу оборудования ПТК.

ЦЕЛЬ ИССЛЕДОВАНИЯ

В данной статье предлагается объединить две методики проверки ПТК [1, 2] для создания улучшенной методики с учетом рекомендаций корпоративного профиля МЭК 61850 ПАО «ФСК ЕЭС» [3]. Данный профиль достаточно четко регламентирует подходы к созданию электронного описания оборудования ПС, использование функционала и коммуникаций в рамках стандарта МЭК 61850. Одним из пунктов усовершенствования методики является вопрос об информационной безопасности в связи с увеличением доли информационного обмена между устройствами, объектами энергетики и т. д. Информационная безопасность предусматривает анализ защищенности ПТК. Такой анализ поможет дополнить и улучшить методику проведения испытаний. Приведенные выше СТО не рассмат-

СТРУКТУРНАЯ СХЕМА ПТК АСУ ТП

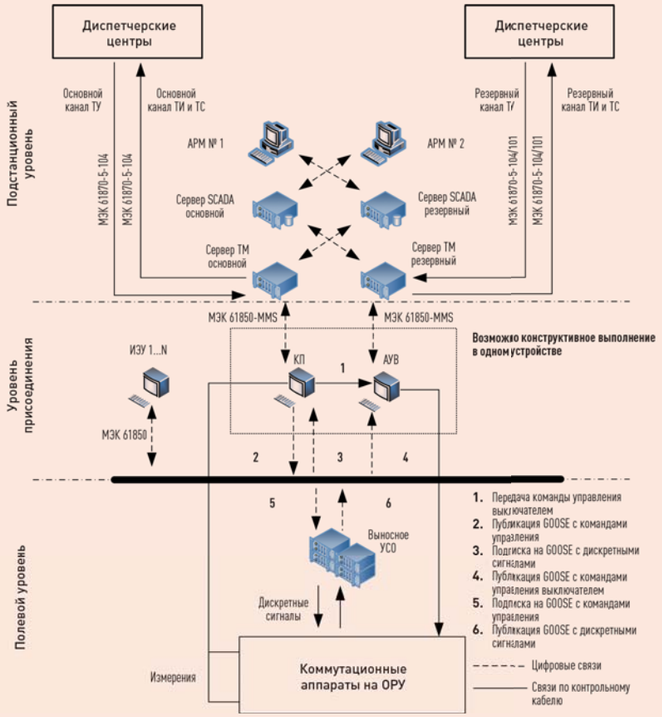


Рис. 1

спроектирован и построен стенд, имитирующий цифровую подстанцию. При построении стенда применялись рекомендации и указания, приведенные в СТО 56947007-25.040.40.226-2016 [4]. Согласно стандарту в ПТК реализуется три уровня программно-технических средств: полевой, уровень присоединения и подстанционный. Такая трехуровневая структура обеспечивает информационное взаимодействие между устройствами, причем уровни функционируют независимо друг от друга, что влияет на степень надежности системы. Такая структура в случае расширения системы не претерпевает особых изменений. Весь процесс будет сводиться к интеграции ИЭУ и установке сетевого подключения.

Структурная схема ПТК АСУ ТП представлена на рис. 1.

Разработанная на основе структуры ПТК АСУ ТП структурная схема полигона ПТК АСУ ТП представлена на рис. 2.

Особенность данного стенда заключается в том, что он очень гибок к расширению оборудования. На нем можно проводить испытания оборудования различных производителей, причем как одиночного элемента, так и всей системы.

СТРУКТУРНАЯ СХЕМА ПОЛИГОНА ПТК АСУ ТП

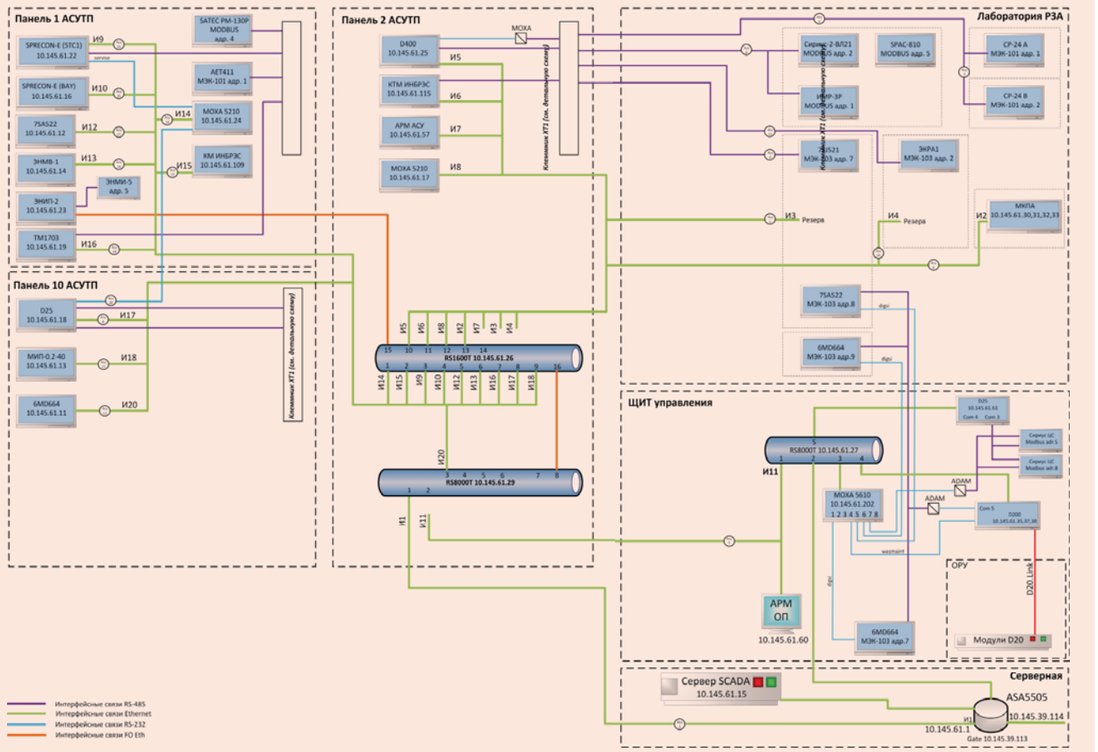


Рис. 2

Оборудование, входящее в состав стенда ПТК АСУ ТП, сконфигурировано по протоколу МЭК 61850. Остальное оборудование на время испытания было отключено от действующей ЛВС. Конфигурация содержит виртуальную машину VM Kali Linux с установленной операционной системой (ОС) для анализа информационной безопасности. С данной ОС производилась DDoS-атака на целевые устройства.

Состав оборудования полигона ПТК АСУ ТП представлен в табл. 1.

На разработанном стенде был проведен ряд экспериментов для исследования характеристик ПТК АСУ ТП в различных режимах. Перед началом испытаний производилась настройка терминалов РЗА и контроллера присоединений (КП). При регулировании количества выдаваемых и регистрируемых сигналов по протоколу MMS с применением циклического GOOSE-сообщения имитировалась загрузка ПТК, тем самым определялись пределы устойчивого функционирования системы, включающие допустимые временные задержки и другие характеристики.

Функциональная схема формирования и прохождения GOOSE-сообщений представлена на рис. 3 на с. 28.

Согласно схеме на рис. 3 контроллер присоединения (ИЭУ1) по нажатию функциональной клавиши генерирует определенное количество N-сигналов по MMS-протоколу и GOOSE-сообщение, которое отправляется на терминал РЗА 7SA522 (ИЭУ2). После приема GOOSE от КП 7SA522 генерирует свое количество сигналов и посылает GOOSE

ривают вопросы информационной безопасности. Поиск уязвимостей системы с помощью атаки целевых устройств с применением эксплоитов (уязвимостей) или атаки на локально-вычислительную сеть (ЛВС) позволит находить наиболее уязвимые места в ПТК, тем самым повышая надежность и безопасность системы при дальнейшей эксплуатации.

ОПИСАНИЕ ОБЪЕКТА ИССЛЕДОВАНИЯ

Для проведения исследований и испытаний ПТК АСУ ТП был

СОСТАВ ОБОРУДОВАНИЯ ПОЛИГОНА ПТК АСУ ТП

№	Наименование	IP адрес
1	Контроллер присоединения ИНБРЭС	10.145.61.115
2	Терминал РЗА 7SA522	10.145.61.12
3	Терминал РЗА 6MD664	10.145.61.11
4	АРМ SCADA с программным обеспечением: – EKRA SCADA Studio – IPerf2 – Wireshark – IEDScout – VM Kali Linux	10.145.61.230
5	Коммутатор RuggedCom RSG2300	10.145.61.26
6	Межсетевой экран (шлюз) CISCO ASA5505	10.145.61.1
7	АРМ АСУ с программным обеспечением: – Transet – Linker 61820 – Digsi 4.90	10.145.61.50

Таблица 1

на 6MD664 (ИЭУ3). 6MD664 также после приема отправления генерирует свои внутренние логические сигналы и GOOSE-посылку на контроллер присоединения. Согласно рис. 3 процесс происходит циклически.

На рис. 4 показан фрагмент логической схемы формирования и генерации N-сигналов по MMS-протоколу, написанной в программе SimBres.

Формирование и генерация N-сигналов по MMS-протоколу производится по нажатию функциональной клавиши [Функция 1] контролера присоединений. Аналогично рис. 4 соблюдается логика программного обеспечения терминалов РЗА. Согласно разработанной программе, испытания проводились при различном количестве сгенерированных N-сигналов в секунду, причем эти испытания для исключения погрешности в замерах проводились с повторением при одних и тех же условиях.

ФУНКЦИОНАЛЬНАЯ СХЕМА ФОРМИРОВАНИЯ И ПРОХОЖДЕНИЯ GOOSE-СООБЩЕНИЙ

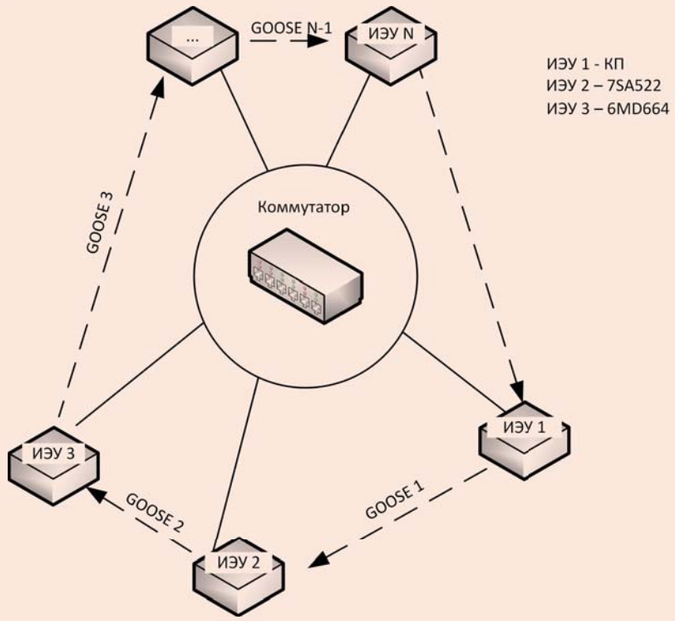


Рис. 3

РЕЗУЛЬТАТЫ ИСПЫТАНИЙ И ИХ ОБСУЖДЕНИЕ

В ходе проведения экспериментов собирались такие показания, как загрузка процессора в долях (CPU) каждого элемента системы, нагрев устройств, задержка при приеме/передаче пакетов с помощью ICMP-протокола, задержки при регистрации сообщений в SCADA. Результаты испытаний для одного присоединения, полученные в ходе трех экс-

ФРАГМЕНТ СХЕМЫ ЛОГИКИ ФОРМИРОВАНИЯ И ГЕНЕРАЦИИ N-СИГНАЛОВ ПО MMS-ПРОТОКОЛУ, НАПИСАННОЙ В SIMBRES

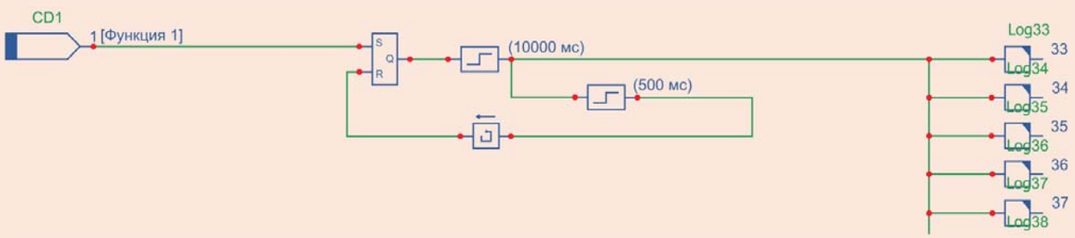


Рис. 4

ГРАФИКИ ЗАГРУЗКИ ПРОЦЕССОРОВ УСТРОЙСТВ ПРИ РАЗЛИЧНОЙ ГЕНЕРАЦИИ СИГНАЛОВ В СЕКУНДУ ДЛЯ ПЕРВОГО ЭКСПЕРИМЕНТА

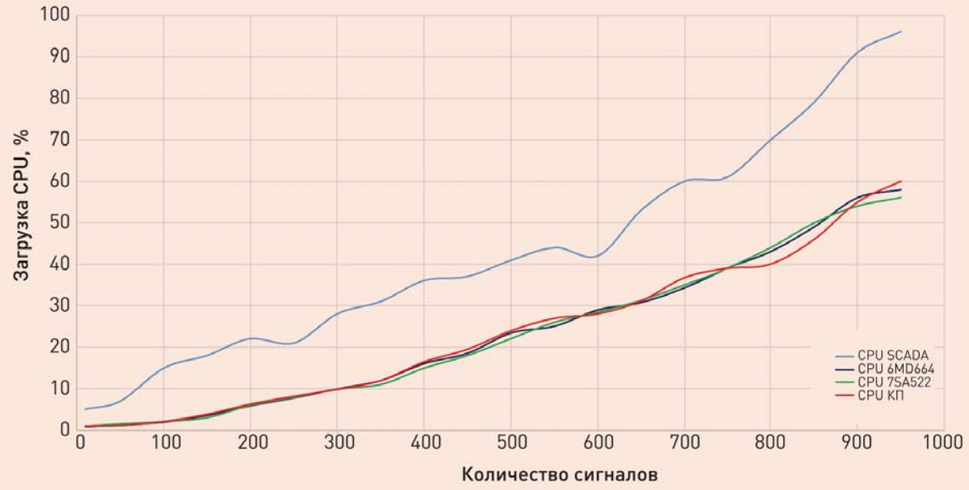


Рис. 5

ГРАФИКИ ЗАГРУЗКИ ПРОЦЕССОРОВ УСТРОЙСТВ ПРИ РАЗЛИЧНОЙ ГЕНЕРАЦИИ СИГНАЛОВ В СЕКУНДУ ДЛЯ ВТОРОГО ЭКСПЕРИМЕНТА

Рис. 6

ГРАФИКИ ЗАГРУЗКИ ПРОЦЕССОРОВ УСТРОЙСТВ ПРИ РАЗЛИЧНОЙ ГЕНЕРАЦИИ СИГНАЛОВ В СЕКУНДУ ДЛЯ ТРЕТЬЕГО ЭКСПЕРИМЕНТА

Рис. 7

периментов, представлены в виде графиков на рис. 5–12.

Как видно из графиков, с увеличением количества генерации сигналов в секунду растет нагрузка на каждый из процессоров. Расхождение результатов связано с температурным режимом. Чем сильнее загрузка на процессор при неизменной тактовой частоте, тем сильнее выделяемое тепло. Графики, соответствующие изменениям температуры для экспериментов 1–3, показаны на рис. 8–10 на с. 31–32.

Как видно из графиков, представленных на рис. 8–10, при увеличении количества сигналов свыше 500 наблюдается рост температуры. Резкое понижение температуры до 35° С свидетельствует об увеличении оборотов кулеров устройства. Можно сделать вывод, что при увеличении температуры выше определенной отметки, сконфигурированной на уровне прошивки устройства, запускается процесс снижения тактовой частоты процессора для снижения вероятности повреждения центрального процессора.

Из-за того, что полигон не располагает большим количеством устройств, было принято решение произвести симуляцию загрузки ЛВС с помощью генерации большого траффика. С помощью ПО iPerf2 на АРМ АСУ был установлен клиентский модуль, который генерировал трафик широковещательными пакетами, а на АРМ SCADA — серверный модуль, который этот трафик получал. Во время генерации трафика одновременно подавались запросы на устройства с помощью команды ping <IPадрес устройства> для проверки временной задержки ответа от устройства. Графики изменения задержки времени отклика устройств при различной генерации сигналов в секунду, полученные в ходе испытаний с применением ICMP-протокола, представлены на рис. 11 на с. 33.

В процессе испытаний регистрировались сообщения по MMS-протоколу в журнал тревог SCADA, скриншот которых представлен на рис. 12 на с. 33.

В результате симуляции увеличения загрузки ЛВС, как показано на рис. 11, наблюдалось увеличение времени задержки ответа от устройств. Одновременно в ходе этой загрузки ЛВС при регистрации MMS в SCADA, как показано на рис. 12, была зафиксирована задержка более 300 мс. Согласно СТО 56947007-25.040.40.226-2016 [4] такая задержка недопустима (задержка не должна превышать 100 мс) для сигналов, связанных с отключением от защит и других критических событий.

ГРАФИК ИЗМЕНЕНИЯ ТЕМПЕРАТУРЫ УСТРОЙСТВ ПРИ РАЗЛИЧНОЙ ГЕНЕРАЦИИ СИГНАЛОВ В СЕКУНДУ ДЛЯ ПЕРВОГО ЭКСПЕРИМЕНТА

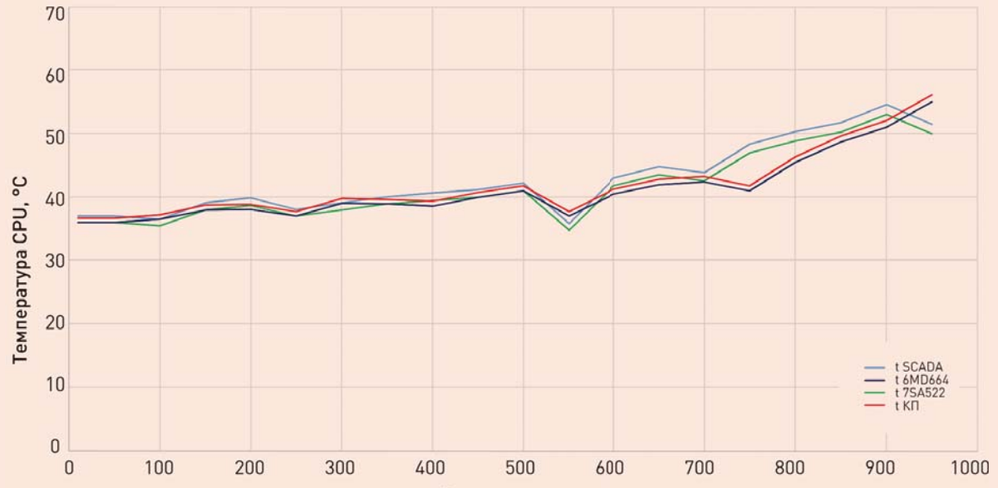


Рис. 8

ГРАФИК ИЗМЕНЕНИЯ ТЕМПЕРАТУРЫ УСТРОЙСТВ ПРИ РАЗЛИЧНОЙ ГЕНЕРАЦИИ СИГНАЛОВ В СЕКУНДУ ДЛЯ ВТОРОГО ЭКСПЕРИМЕНТА

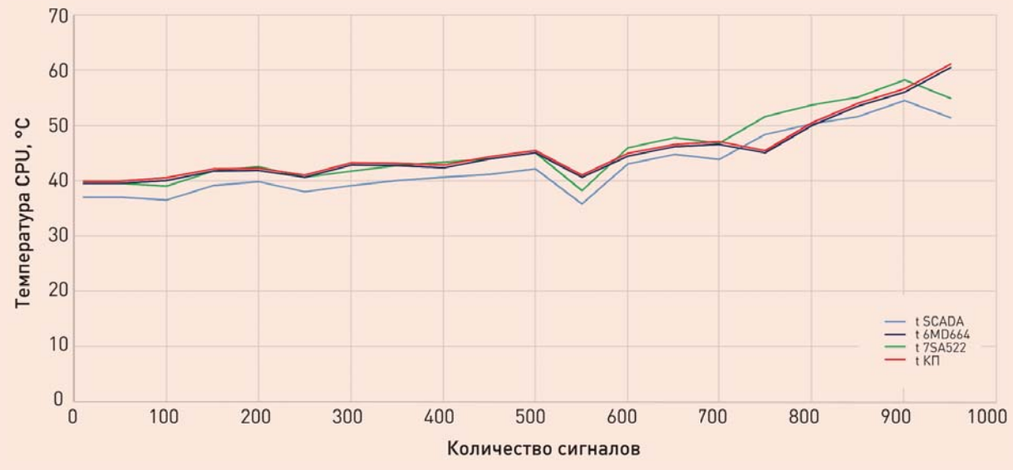


Рис. 9

ГРАФИК ИЗМЕНЕНИЯ ТЕМПЕРАТУРЫ УСТРОЙСТВ ПРИ РАЗЛИЧНОЙ ГЕНЕРАЦИИ СИГНАЛОВ В СЕКУНДУ ДЛЯ ТРЕТЬЕГО ЭКСПЕРИМЕНТА

Рис. 10

Для уменьшения задержек времени на электроэнергетических объектах может применяться принцип сегментирования сети, который заключается в создании виртуальной локальной сети (VLAN) для каждого типа трафика или устройств, например, VLAN 1 — для MMS-сообщений, VLAN 2 — для GOOSE-сообщений и т. п. С увеличением количества ИЭУ и, как следствие, увеличением информационного облака использование сегментирования позволит отфильтровать трафик, протекающий внутри подстанции или станции и разгрузить ЛВС [5].

Следующим испытанием была имитация проведения атаки на открытый порт целевого устройства при помощи DDoS-атаки. Проверка заключалась в отправке от источника тысяч пакетов с рандомными адресами [6]. В общем случае ее можно охарактеризовать как проверку на защищенность и устойчивость ПТК к подобным атакам. В результате атаки устройство, имеющее открытый порт, прекращало функционировать. Загрузка процессора достигала 100 %. При атаке на АРМ наблюдались не только загрузка ЦП и полное поглощение оперативной памяти, но и возрастание нагрузки на жесткий диск. Такое воздействие впоследствии приведет к ускорению износа жесткого диска.

На практике наладчики обычно не настраивают сетевое оборудование. Для объектов с десятками устройств, не использующих сегментирование, в случае развития крупной нештатной ситуации вероятность потери аварийных сигналов крайне высока.

ЗАКЛЮЧЕНИЕ

Таким образом, можно сделать вывод, что во время испытания ПТК АСУ ТП и/или ССПИ, согласно СТО 56947007-25.040.40.112-2011, необходимо учитывать много факторов, и результат напрямую зависит от количества ИЭУ и сетевого оборудования [7]. Данные испытания невозможно провести на действующем объекте, хотя некоторые пункты программы рекомендуются для проведения технического обслуживания на объектах или при проведении испытаний ПТК в случае его расширения. Основываясь на полученных результатах, необходимо включать в проверку ПТК АСУ ТП и/или ССПИ, а в их испытания — исследование влияния нагрузочных режимов оборудования. Исследования подтверждают, что результат проведения испытаний, согласно СТО 56947007-25.040.40.112-2011 [1], зависит от того, насколько оборудование загружено и насколько долго оно находилось под воздействием нагрузки. Проведение анализа системы инструментами информационной безопасности позволяет выявить наиболее уязвимый участок еще до ввода в опытную эксплуатацию оборудования или до проведения испытаний, тем самым повышая

ГРАФИК ИЗМЕНЕНИЯ ЗАДЕРЖКИ ВРЕМЕНИ ОТКЛИКА УСТРОЙСТВ ПРИ РАЗЛИЧНОЙ ГЕНЕРАЦИИ СИГНАЛОВ В СЕКУНДУ ПРИ ПРИМЕНЕНИИ ICMP-ПРОТОКОЛА

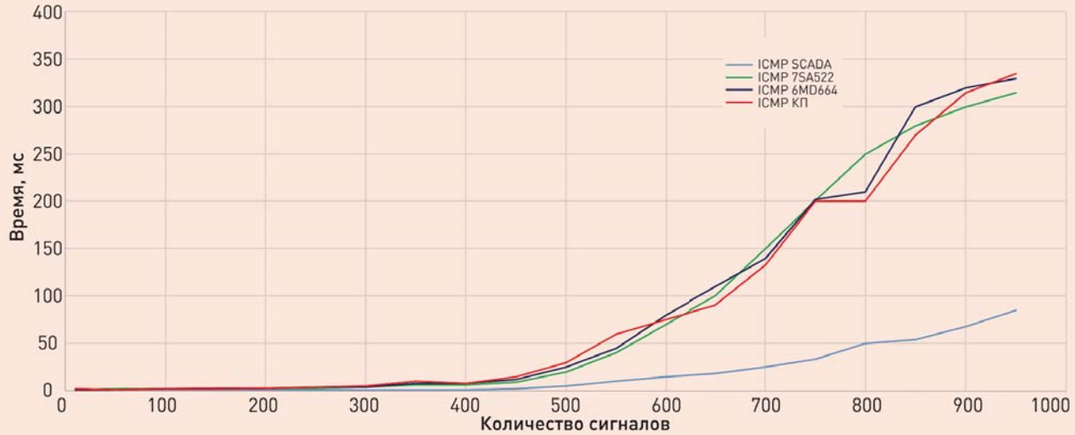


Рис. 11

надежность всей системы. Проверка системы информационной нагрузкой и применение программного обеспечения в области информационной безопасности можно рекомендовать для проведения технического обслуживания ПТК АСУ ТП и/или ССПИ на действующих объектах.

СКРИНШОТ ЖУРНАЛА ТРЕВОГ SCADA

AC	07.02.2019 03:37:00.625	ЦПП, 7SA		Дискретный сигнал 9	Срабатывание
AC	07.02.2019 03:37:00.625	ЦПП, 7SA		Дискретный сигнал 8	Срабатывание
AC	07.02.2019 03:37:00.625	ЦПП, 7SA		Дискретный сигнал 6	Срабатывание
AC	07.02.2019 03:37:00.625	ЦПП, 7SA		Дискретный сигнал 20	Срабатывание
AC	07.02.2019 03:37:00.625	ЦПП, 7SA		Дискретный сигнал 18	Срабатывание
AC	07.02.2019 03:48:22.969	ЦПП, 6MD		Дискретный сигнал 4	Срабатывание
AC	07.02.2019 03:48:22.969	ЦПП, 6MD		Дискретный сигнал 3	Срабатывание
AC	07.02.2019 03:48:22.969	ЦПП, 6MD		Дискретный сигнал 5	Срабатывание
AC	07.02.2019 03:48:22.969	ЦПП, 6MD		Дискретный сигнал 2	Срабатывание
AC	07.02.2019 03:48:22.969	ЦПП, 6MD		Дискретный сигнал 6	Срабатывание
AC	07.02.2019 03:48:23.069	ЦПП, 6MD		Дискретный сигнал 31	Срабатывание
AC	07.02.2019 03:48:23.069	ЦПП, 6MD		Дискретный сигнал 50	Срабатывание

Рис. 12

ЛИТЕРАТУРА

1. СТО 56947007-25.040.40.112-2011. Типовая программа и методика испытаний программно-технического комплекса автоматизированной системы управления технологическими процессами (ПТК АСУ ТП) и микропроцессорного комплекса системы сбора и передачи информации (МПК ССПИ) подстанций в режиме повышенной информационной нагрузки «шторм». Стандарт организации ОАО «ФСК ЕЭС», 2011. 68 с.
2. СТО 56947007-25.040.40.160-2013. Типовая программа и методика заводских испытаний программно-технических комплексов автоматизированных систем управления технологическими процессами, систем сбора и передачи информации (ПТК АСУ ТП и ССПИ). Стандарт ПАО «ФСК ЕЭС», 2013. 67 с.
3. Корпоративный профиль МЭК 61850 ПАО «ФСК ЕЭС». Стандарт организации ПАО «ФСК ЕЭС», 2018.
4. СТО 56947007-25.040.40.226-2016. Типовые технические требования к функциональной структуре автоматизированных систем управления технологическими процессами подстанции Единой национальной электрической сети. Стандарт организации ПАО «ФСК ЕЭС», 2016. 60 с.
5. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов. 5-е изд. СПб.: Питер, 2017. 992 с.
6. Ресурс об обеспечении информационной безопасности «Codeby.net». [Электронный ресурс]. URL: http://codeby.net/ (дата обращения 20.01.2019).
7. Аномем Ю., Ли Х., Кроссли П., Жанг Р., МакТаггерт К. Количественная оценка надежности различных архитектур шины процесса по МЭК 61850 // Релейщик, 2012. № 1. С. 48–52.