УДК 007.51:004.056:004.274

С.Я. Гильгурт, г. Киев

АНАЛИЗ ПРИМЕНЕНИЯ АППАРАТНОГО УСКОРЕНИЯ ИНФОРМАЦИОННОЙ ЗАЩИТЫ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ЭНЕРГЕТИЧЕСКОЙ ОТРАСЛИ

Abstract. Application of FPGA-based acceleration of security tasks in power grid is analyzed. SCADA-systems, smart grid, protocols of IEC 61850, NIDS, regular expressions and Extended Shift-And algorithm for this purpose are investigated.

Введение

Использование достижений информационных технологий при автоматизации производственных процессов предоставляет множество преимуществ, таких как стандартизация, проработанность технических решений, относительно невысокая стоимость. Вместе с тем применение IT-подходов при построении АСУ ТП и систем автоматики привносит и присущие им недостатки, включая проблемы информационной безопасности. Причем, последствия от реализации угроз в данной сфере могут быть более тяжелыми по сравнению с традиционными областями применения информационных технологий, особенно при автоматизации объектов критической инфраструктуры, к которой относится энергетическая отрасль.

Правительственные организации и отраслевые специалисты начинают осознавать опасность нанесения катастрофического ущерба стране кибератаками на объекты критической инфраструктуры. Популярный ранее принцип "Безопасность через неясность" ("Security through obscurity"), заключающийся в достижении информационной безопасности путем сокрытия внутреннего устройства системы и особенностей ее реализации, уже не отвечает реалиям времени. Это наглядно продемонстрировали подтвержденные атаки с применением червя Stuxnet на иранские объекты атомной промышленности в 2010-м году и троянской программы BlackEnergy – на энергопоставляющие предприятия Украины в 2015-ом [1].

В научной литературе появляется все больше публикаций, посвященных анализу и разработкам в области информационной защиты систем автоматизации. Однако, как признают сами исследователи, ситуация пока еще остается на начальном этапе. В этой связи вопросы анализа особенностей и повышения эффективности решения задач информационной безопасности применительно к автоматизированным и автоматическим системам управления в энергетике являются актуальными и злободневными.

Целью данной работы является исследование систем автоматизации в энергетической отрасли, в первую очередь – электроэнергетики, на предмет применимости реконфигурируемых аппаратных ускорителей для эффективного решения задач информационной безопасности.

1. Информационная безопасность SCADA-систем

С развитием микропроцессорной техники мир управления промышленным производством вообще, и энергетикой в частности, быстро перешел на цифровую основу. В области управления крупными техническими предприятиями стандартом де-факто стали системы диспетчерского управления и сбора данных – так называемые SCADA-системы (от английского Supervisory Control And Data Acquisition) [2, 3]. Архитектурно такие системы состоят из двух уровней; на верхнем предполагается наличие некоторого главного узла MTU (Master Terminal Unit); на нижнем – множество подконтрольных удаленных узлов RTU (Remote Terminal Unit). Уровни объединяются в единую структуру посредством коммуникационной системы CS (Communication System). MTU характеризуется наличием развитых средств человеко-машинного интерфейса HMI (Human Machine Interface). В качестве RTU могут выступать программируемые логические контроллеры PLC (programmable logic controller) либо устройства связи с объектом (УСО), которые обеспечивают передачу данных с датчиков (дискретных либо аналоговых) и выдачу управляющих воздействий на исполнительные устройства.

Следует заметить, что в русско-/украиноязычной и англоязычной литературе устоялось несколько различное толкование термина SCADA-система [4]. Если в русском/украинском языке под ним чаще понимают программный продукт, используемый на верхнем уровне (такой как In Touch, iFIX, Factory Link, WinCC, Trace Mode и т.п.), то в английском – систему автоматизации в целом, реализованную согласно архитектуре SCADA. В данной работе будем придерживаться англоязычного (более общего) толкования данного термина.

Изначально SCADA-системы имели мало общего со средствами информационно-коммуникационной индустрии – локальными и глобальными сетями, интернет-инфраструктурой – как в функциональном плане, так и по используемым технологиям. Связь с удаленными объектами осуществлялась по так называемым полевым шинам, использующим специфические промышленные протоколы передачи данных. Информационные каналы связи SCADA-систем были отделены от Глобальной сети. Поэтому в те времена основное внимание уделялось физической защите систем управления, в смысле кибернетических угроз они считались безопасными.

Однако со временем ситуация изменилась. Разнородные и несовместимые между собой полевые шины начал вытеснять универсальный стандарт Industrial Ethernet. Внутренние коммуникационные связи размножились и усложнились. Появлялись новые подходы и технические решения. Так, в области электроэнергетики возникло направление Smart Grid. Образующие его подсистемы, помимо традиционных SCADA-систем, такие как Wide Area Monitoring Protection and Control (WAMPAC), Distribution Management System (DMS), Advanced Metering Infrastructure (AMI) и коммуникационные структуры более высокого уровня, использующие

интранет-технологии, стали более уязвимыми в плане кибербезопасности. А доступ в интернет настолько упростился, что гарантировать полную независимость информационной инфраструктуры энергетических объектов от всемирной сети стало практически невозможно [5].

2. Автоматизация электрических подстанций. Стандарт МЭК-61850

Электрические подстанции являются одними из самых многочисленных объектов энергетики. От их надежной работы в значительной степени зависит стабильная и бесперебойная подачи электроэнергии потребителям [5]. Неизбежный процесс автоматизации и перевода на цифровую элементную базу подстанций энергетических компаний по всему миру за последние годы сталкивается с объективными трудностями. Если жизненный цикл силового оборудования, такого как разъединители, составляет порядка 40 лет, то управляющие системы обновляются в среднем лет через 15. Типична ситуация, когда в едином комплексе соседствуют устройства нескольких поколений, не совместимые между собой. Использование преобразователей для состыковки разных стандартов и протоколов приводит к замедлению работы системы, повышает риск возникновения ошибок, снижая тем самым надежность сетей электроснабжения.

Для решения проблемы был разработан стандарт МЭК-61850 «Сети и системы связи на подстанциях» [6]. Целью его создания было предложить единые правила для построения электрических подстанций. Правила, которые бы, с одной стороны, защищали инвестиции в энергетику, с другой – позволяли в будущем использовать самые передовые вычислительные и коммуникационные технологии, не затрагивая при этом форматы данных и структуру управления оборудованием. Документ, первая редакция которого появилась в 2003 году, включает в себя целый набор стандартов – по одноранговой и клиент-серверной связи, по структуре и конфигурации подстанции, по методике испытаний, экологическим требованиям, проектированию и т.п.

Комплекс нормативов МЭК-61850 представляет собой довольно объемный документ, состоящий из более десяти подразделов. И продолжает развиваться. Тем не менее, на сегодняшний день у специалистов он однозначно ассоциируется с понятием "цифровая подстанция". Что, кроме прочего, подразумевает использование цифровых измерительных приборов вместо аналоговых, а также применение интеллектуальных электронных устройств, обозначаемых в англоязычной литературе аббревиатурой IED (Intelligent Electronic Devices).

В Украине передовое энергетическое оборудование класса smart grid на базе МЭК-61850 только начинает внедряться. Так в 2018 году планируется, оснастить цифровой подстанцией Приморскую ветроэлектростанцию в Запорожской области [7]. Но, для успешного решения вопросов кибербезопасности необходимо их учитывать заранее, на стадиях планирования и проектирования.

Помимо единообразия форматов данных и правил обмена, пакет нормативов МЭК-61850 стандартизует также коммуникационные протоколы. С этой целью в качестве единого средства передачи информации на всех уровнях подстанции выбрана сеть Ethernet. Данная технология обеспечивает обратную совместимость всех своих версий, начиная 70-х годов прошлого века. Интерфейс Ethernet, используемый на всех уровнях автоматизации, предоставляет ряд преимуществ. Он стандартизует, удешевляет и упрощает кабельные соединения, облегчает проектирование, тестирование и обучение персонала. С другой стороны, пакетная передача данных и основанные на ней вышестоящие протоколы делают цифровые подстанции, которые являются объектами критической инфраструктуры, потенциально уязвимыми для кибератак. [8 – 12].

3. Особенности информационной защиты киберфизических систем по сравнению с информационно-коммуникационным объектами

В связи с тем, что повышенный уровень кибернетических угроз привнесен в область промышленной автоматизации из сферы IT-технологий, возникает естественный вопрос – насколько наработанный там опыт киберзащиты применим для промышленных систем (которые называют киберфизическими, чтобы подчеркнуть отличие от систем информационно-коммуникационных)? Насколько различаются подходы к защите информации, применимые в этих двух областях.

На основе анализа литературы попробуем проанализировать и оценить степень этого различия.

Последние исследования свидетельствуют, что существующая в IT-сфере методология борьбы с киберугрозами не в полной мере применима для SCADA-систем на базе стандарта МЭК-61850 [1]. Среди аргументов приводятся тот факт, что цифровые устройства, используемые в том же smart grid, равно как и в SCADA-системах, обладают ограниченными вычислительными ресурсами. Построены они зачастую на устаревшей по меркам IT-индустрии элементной базе. Традиционные приемы кибербезопасности плохо применимы в таких устройствах, поскольку для них трудно обновлять ПО и firmware, использовать традиционные антивирусы, программные межсетевые экраны [5]. Системы обнаружения вторжений (СОВ), особенно реализованные программно для традиционных компьютеров, также недостаточно эффективны применительно к промышленным сетям [13].

С другой стороны, ряд экспертов отмечают и противоположную тенденцию, заключающуюся в том, что традиционные инструменты киберзащиты, в частности, системы обнаружения вторжений, не только возможно и необходимо задействовать в промышленной автоматизации, правда, существенно доработанные с учетом ее специфики.

Так, исследователи отмечают, что, несмотря на наличие в стандарте МЭК встроенных механизмов безопасности, предусмотренных документами

МЭК-62351-4 и МЭК-62351-6 [14], неизменный рост активности и изобретательности злоумышленников требует применения все более гибких и адаптивных средств киберзащиты [9]. Тем более что, как отмечают другие авторы, большинство производителей устройств IED не в полной мере реализуют в своих изделиях функции безопасности, предписываемые стандартом [1].

Говоря об особенностях и специфике киберзащиты систем промышленной автоматики, упоминают возможность и необходимость в процессе распознавания вредоносной активности учитывать физическую инфраструктуру. В то время как традиционные IT-коммуникации являются существенно гетерогенными и в широких пределах варьируются по своей природе, киберфизические системы обладают определенной структурой и типовыми шаблонами коммуникации, которые следует принимать в расчет при обнаружении подозрительной активности [1].

Отметим, что фактор учета структурной специфики следует рассматривать скорее как преимущество промышленных систем перед информационными объектами в плане защиты информации. Наиболее наглядно оно может быть проиллюстрировано на следующем примере. Если в трафике между двумя конкретными узлами промышленной сети согласно структуре информационных обменов должны присутствовать пакеты лишь конкретных протоколов, то система обнаружения вторжений имеет основания интерпретировать любые другие пакеты как заведомо злонамеренные и выдавать предупреждение о вторжении [5].

Позитивным моментом можно считать также тот факт, что с целью повышения быстродействия в ряде протоколов, применяемых в киберфизических системах, прикладной уровень взаимодействует напрямую с канальным, минуя промежуточные уровни сетевой модели OSI. На рис. 1 ([1]) схематически изображены стеки промышленных протоколов MMS (Manufacturing Message Specification), SMV (Sampled Measure Value) и протокола обмена сообщениями GOOSE (Object Oriented Substation Event), а также традиционный для IT протокол синхронизации времени SNTP. Очевидно, что в сетевых соединениях, задействующих лишь промышленные протоколы SMV и GOOSE, наличие любых пакетов с представительского по сетевой включительно будет свидетельствовать о ненормальной активности.

4. Системы обнаружения вторжений для цифровых электрических подстанций

Рассмотренные выше особенности организации киберзащиты в промышленных сетях могут быть использованы в качестве основы для создания систем обнаружения вторжений для интеллектуальных подстанций на базе стандарта МЭК-61850. И подобные СОВ уже начинают появляться [12, 15 – 17]. Однако, как отмечают исследователи, они находятся пока на начальной стадии разработки [1].

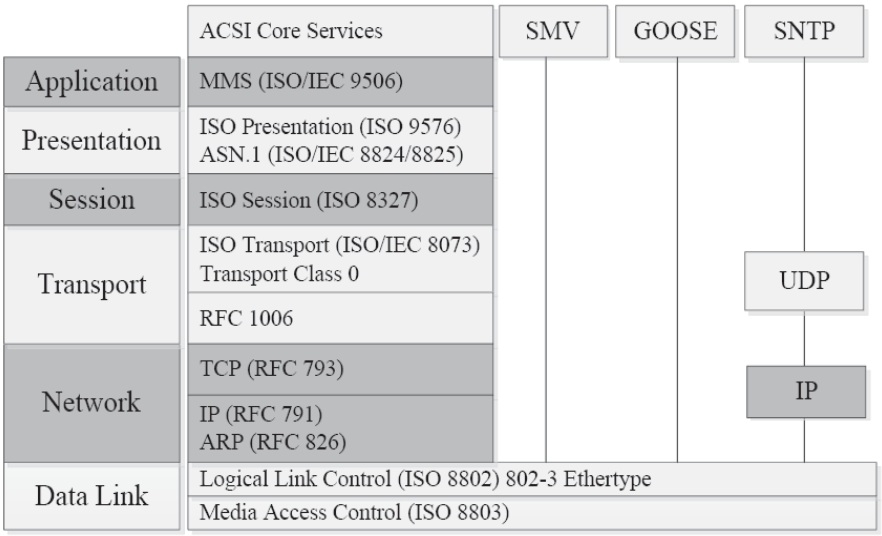

Рис. 1. Протоколы стандарта МЭК-61850

Рассмотрим, каким образом система обнаружения вторжений может быть включена в состав цифровой подстанции.

Наиболее простым и эффективным решением является включить СОВ в состав маршрутизатора между сетями SCADA-системы и подстанции (рис. 2) [9]. В этом случае контролируется весь входящий в сеть smart grid трафик.

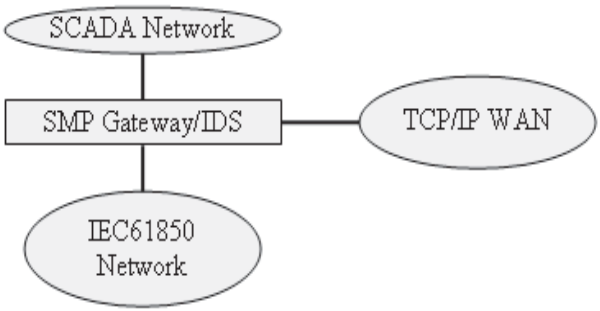

Рис. 2. СОВ (IDS) в составе маршрутизатора (Gateway)

Если по каким-либо причинам такой вариант невозможен, СОВ включают сразу после маршрутизатора (рис. 3) [9].

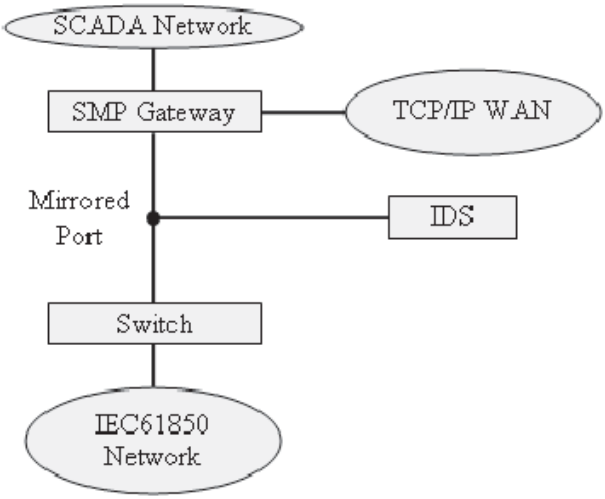

Рис. 3. СОВ (IDS) вне маршрутизатора (Gateway)

Использование встроенных систем обнаружения вторжений (host-based) в промышленных сетях нецелесообразно в силу упомянутых выше ограничений цифровых устройств по вычислительным ресурсам.

5. Использование регулярных выражений для распознавания атак на протоколы smart grid

Как известно, системы обнаружения вторжений по принципу распознавания можно разделить на использующие сигнатуры (Signature-based IDS) и выявляющие аномалии (Anomaly based IDS) [18]. Сигнатурные СОВ в качестве недостатка обладают свойством невозможности распознавать вновь появившиеся атаки, не внесенные еще в базу образцов системы. Однако решения на основе аномалий все еще демонстрируют недопустимо высокий уровень ошибок распознавания первого, а особенно много - второго рода. По этой причине на практике наиболее распространены системы на базе сигнатур.

В данном контексте сигнатура – описание конкретной атаки (злонамеренной активности), позволяющее однозначно ее идентифицировать. В простейшем случае оно представляет собой фиксированную последовательность (строку) символов определенной длины. Однако во многих случаях характерные признаки одной и той же атаки могут варьироваться в широких пределах, в результате чего сигнатура превращается в совокупность большого числа различных комбинаций из подстрок и отдельных символов. При этом общее количество возможных вариантов написаний одной и той же сигнатуры может достигать астрономически больших значений.

В таких случаях в качестве технически реализуемого решения используют механизм так называемых регулярных выражений (regular expression). Подход позволяет путем дополнительного использования специальных символов-джокеров (wild card) задать некий шаблон, описывающий одновременно множество строк. Например, символ точки ("."), входящий в шаблон в качестве джокера, может обозначать один произвольный символ; несколько символов, перечисленных через запятую внутри пары квадратных скобок ("[,]") – один из символов списка; символ вопросительного знака ("?"), стоящий рядом с подшаблоном – как наличие, так и отсутствие данного подшаблона в искомой сигнатуре; пара чисел в фигурных скобках ("{m, n}") – число допустимых повторов подшаблона в интервале от m до n, и т.п.

Существует несколько различных языков описания регулярных выражений. Применительно к системам обнаружения вторжений наибольшее распространение получил формат, совместимый с языком Perl (широко используемом в UNIX-подобных ОС для решения системных задач) – PCRE (Perl Compatible Regular Expressions) [19, 20]

Примером сигнатуры, описывающей атаку на протокол сообщений GOOSE, используемый в цифровых электрических подстанциях, автоматизированных согласно стандарту МЭК-61850, может служить регулярное выражение [8]

$$\mathbf{RE = GOOSEID.\{0, 20\}[\backslash x50 - \backslash x58]} \quad (1)$$

Такая сигнатура описывает подстроку "GOOSEID", за которой через произвольное количество от 0 до 20 произвольных символов следует число в диапазоне от 80 (50_{16}) до 88 (58_{16}). Обнаружение описанной таким образом последовательности символов в поле Application Protocol Data Unit (APDU) пакета Ethernet в комбинации с MAC-адресом передающей станции позволяет распознать сетевую атаку с использованием сообщений протокола GOOSE, применяемого в подстанциях для критических по времени операций. При отправке пакета со значением числа (TAG) равным 84 с устройства с конкретным MAC-адресом, полученные пакеты с адресом, не входящим в перечень предопределенных MAC-адресов, запрещены и должны быть заблокированы [8].

6. Реализация на базе ПЛИС промышленной системы обнаружения вторжений

В работе [8] приведено описание сетевой системы обнаружения вторжений (NIDS) на базе программируемой логических интегральных схем (ПЛИС) типа FPGA, ориентированной на работу с сообщениями протокола GOOSE промышленной сети электрических подстанций. Существует множество технических решений построения распознающего модуля СОВ на

базе программируемой логики, в том числе – с применением регулярных выражений. [21]. В данной работе используется модификация расширенной версии алгоритма Домёлки–Бейза-Ятса–Гоннета, (Есть сведения, что впервые описание алгоритма было опубликованного еще в 1965 г. [22]) Однако авторы используют менее корректное, но более распространенное в англоязычной литературе название Shift-And-алгоритм. Расширенная версия алгоритма (ESA – Extended Shift-And algorithm) предложена в 2002 году Навarро и Раффинотом [23].

На рис. 4 приведена таблица переходов цифрового автомата распознающего модуля СОВ на базе алгоритма ESA для идентификации регулярного выражения (1) [8].

Transition table: $RE = GOOSEID.\{0, 20\}[\backslash x50\text{-}\backslash x58]$.

Bit position	1	2	3	4	5	6	7	8	9
Init	1	0	0	0	0	0	0	0	0
Accept	0	0	0	0	0	0	0	0	1
Move[D]	0	0	0	0	0	0	1	1	0
Move[E]	0	0	0	0	1	0	0	1	0
Move[G]	1	0	0	0	0	0	0	1	0
Move[I]	0	0	0	0	0	1	0	1	0
Move[O]	0	1	1	0	0	0	0	1	0
Move[S]	0	0	0	1	0	0	0	1	0
Move[\x50-\x58]	0	0	0	0	0	0	0	1	1
Move[.]	0	0	0	0	0	0	0	1	0
Repeat[.]	0	0	0	0	0	0	0	1	0
START	0	0	0	0	0	0	1	0	0
END	0	0	0	0	0	0	0	1	0
SPACE	0	0	0	0	0	0	1	1	0
CR	0	0	0	0	0	0	0	1	0

Рис. 4. Таблица переходов цифрового автомата распознающего модуля СОВ

Разработка практически реализована на ПЛИС Zynq-7030 от производителя Xilinx. Проект занял 43080 поисковых таблиц (LUT), что составило 54,81% от их общего числа, а также все блоки встроенной памяти (BRAM) кристалла; для хранения данных счетчика задействована внешняя память RAM. При этом достигнута максимальная рабочая частота в 133,35 МГц, что соответствует пропускной способности в 1066 Гбит/сек [8].

Выводы

В работе предпринята попытка проанализировать различия в подходах к реализации киберзащиты для IT-сферы и систем промышленной автоматизации электроэнергетических объектов.

С этой целью кратко рассмотрен широкий круг тем, включающий: SCADA-системы, Smart Grid, устройства IED, стандарт МЭК-61850 и некоторые его протоколы, системы обнаружения вторжений, регулярные выражения и алгоритм Домёлки–Бейза-Ятса–Гоннета.

Главный вывод, который может быть получен по результатам исследования, заключается в том, что состояние дел по проблеме информационной защиты современных промышленных объектов на сегодняшний день находится на начальной стадии.

Выяснилось также, что киберфизические системы, к которым относятся в частности современные цифровые подстанции, требуют иных подходов при создании систем киберзащиты. Выявлено противоречие, суть которого сводится к тому, что имеющийся в IT-области опыт борьбы с кибератаками, с одной стороны, не применим напрямую к интеллектуальным промышленным системам, с другой – его целесообразно использовать, но с обязательным учетом ряда существенных поправок.

Наконец, обнаружены особенности, предоставляющие некоторые преимущества киберфизических систем перед массовыми информационно-коммуникационными приложениями в плане киберзащиты.

Найдена, как минимум, одна ниша, в которой могут быть успешно применены (и уже применяются) аппаратные ускорители на базе ПЛИС. Свойство реконфигурируемости таких решений отвечает упоминавшимся требованиям высокой гибкости и адаптивности средств информационной защиты систем промышленной автоматики.

1. *Yang Y., Xu H.-Q., Gao L., Yuan Y.-B., McLaughlin K., Sezer S.* Multidimensional intrusion detection system for IEC 61850-based SCADA networks, IEEE Trans. Power Deliv. Vol. 32, pp.1068–1078, 2017.
2. *Андреев Е.Б., Куцевич Н.А., Синенко О.В.* SCADA-системы: взгляд изнутри. – М.: РТСофт, 2004. – 176 с.
3. *Boyer S.A.* SCADA: Supervisory Control and Data Acquisition, International Society of Automation USA, 4th Edition, 2009. – 179 p.
4. *Кавалеров М.В.* К вопросу о термине «SCADA-Система» // Вестник ПГТУ. Электротехника, информационные технологии, системы управления. – 2011. – № 5. – С.205-209.
5. *Yang Y., McLaughlin K., Sezer S., Littler T., Im E.G., Pranggono B., Wang H.F.* Multi-Attribute SCADA-Specific Intrusion Detection System for Power Networks, IEEE Trans. on Power Delivery, vol. 29, pp.1092-1102, 2014.
6. Communication Networks and Systems in Substations, IEC Std. 61850, 2003.
7. Первая в Украине инновационная цифровая подстанция в скором времени заработает в Запорожье / UKRINFORM. ультимедийная платформа иновещания Украины [Электронный ресурс]. – Режим доступа: https://www.ukrinform.ru/rubric-economy/2489017-pervaa-v-ukraine-innovacionnaa-cifrovaa-podstancia-v-skorom-vremeni-zarabotaet-v-zaporoze.html – Загл. с экрана. – (Дата обращения: 07.08.2018).]
8. *Kim J., Park J.* FPGA-based network intrusion detection for IEC 61850-based industrial,

Elesevier ICT Express, vol. 4, pp.1-5, 2018.
9. *Premaratne U.K., Samarabandu J., Sidhu T.S., Beresh R., Tan J.-C.* An intrusion detection system for IEC61850 automated substations, IEEE Trans. Power Deliv., vol. 25, pp.2376–2383, 2010.
10. *Hong J., Liu C.-C., Govindarasu M.* Detection of cyber intrusions using network-based multicast messages for substation automation, in: Innovative Smart Grid Technologies Conference, ISGT, IEEE PES, 2014, pp.1-5.
11. *Rashid M.T.A., Yussof S., Yusoff Y., Ismail R.* A review of security attacks on IEC61850 substation automation system network, in: Proceedings of the 6th International Conference on Information Technology and Multimedia, 2014, pp.5-10.
12. *Moreira N., Molina E., Lázaro J., Jacob E., Astarloa A.* Cybersecurity in substation automation systems, Renewable and Sustainable Energy Reviews, vol. 54, 2016, pp.1552-1562.
13. *Premaratne U., Samarabandu J., Sidhu T., Beresh B., Tan J.C.* Evidence theory based decision fusion for masquerade detection in IEC61850 automated substations. International Conference on In-formation and Automation for Sustainability, 2008, pp.194-199.
14. Power Systems Management and Associated Information Exchange – Data and Communications Security. IEC Std. 62351.
15. *Sridhar S., Hahn A., Govindarasu M.* Cyber-Physical System Security for the Electric Power Grid, IEEE Proc., vol. 100, pp. 210-224, Jan. 2012.
16. *Liu C.-C., Stefanov A., Hong J., Panciatici P.* Intruders in the Grid," IEEE Power Energy Magazine, vol. 10, pp. 58-66, Jan. 2012.
17. Hadeli H., Schierholz R., Braendle M., Tuduce C. Generating configuration for missing traffic detector and security measures in industrial control systems based on the system description files, in Proc. 2009 IEEE Conf. on Technologies for Homeland Security, pp.503-510.
18. *.Коростиль Ю.М., Гильгурт С.Я.* Принципы построения сетевых систем обнаружения вторжений на базе ПЛИС // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ ім Г.Є. Пухова НАН України. – Вип. 57. – К.: 2010. – С.87-94.
19. PCRE – Perl Compatible Regular Expressions [Электронный ресурс]. – Режим доступа: http://www.pcre.org. – Загл. с экрана. – (Дата обращения: 07.08.2018).
20. *Коростиль Ю.М., Гильгурт С.Я., Назаренко О.М.* Анализ базы данных системы информационной безопасности Snort и вопросы быстродействия // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ ім. Г.Є. Пухова НАН України. – Київ, 2012. – Вип. 66. – С.77-84.
21. *Давиденко А.Н, Гильгурт С.Я.* Алгоритмы распознавания строк в системах обнаружения вторжений на ПЛИС // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ ім. Г.Є. Пухова НАН України. – Київ, 2010. – Вип. 58. – С. 103–109.
22. *Смит Б.* Методы и алгоритмы вычислений на строках. / Пер. с англ. – М.: Вильямс, 2006. – 496 с.
23. *Navarro G., Raffinot M.* Flexible Pattern Matching in Strings: Practical On-Line Search Algorithms for Texts and Biological Sequences, Cambridge University Press, Cambridge, 2002.

Поступила 1.03.2018р.