Научная статья

УДК 004.4’2, 004.49, 681.5, 004.056.53
DOI 10.25205/1818-7900-2021-19-4-5-15

Методы защиты команд управления в инструментальной среде для автоматизированных систем управления технологическими процессами

Анатолий Иванович Благодарный [1]
Борис Николаевич Пищик [2]

[1, 2] Федеральный исследовательский центр информационных и вычислительных технологий
Новосибирск, Россия

[2] Новосибирский государственный университет
Новосибирск, Россия

[1] ablagodarnyj@mail.ru, https://orcid.org/0000-0001-8668-1094
[2] pishchik.boris@ya.ru, https://orcid.org/0000-0001-9083-4807

Аннотация

Рассматриваются методы, обеспечивающие выполнение только корректных и легальных команд управления в автоматизированных системах управления технологическими процессами (АСУ ТП). Защита целостности программного обеспечения АСУ ТП на всех узлах технологической сети, включая защиту от несанкционированной подмены, осуществляется проверкой контрольных параметров программного обеспечения во время запуска. Защита команд управления от искажений в процессе передачи по сети реализуется двухкратным кодированием на разных уровнях системы. Защита от подачи на технологическое оборудование несанкционированных команд управления осуществляется посредством распознавания этих команд в подсистеме нижнего уровня и сравнением их текущих характеристик с контрольными.

Определенный вклад в безопасность работы АСУ ТП вносит использование безопасной среды исполнения – ОС CentOS 7.

Ключевые слова

АСУ ТП, SCADA, методы защиты, команды управления

Для цитирования

Благодарный А. И., Пищик Б. Н. Методы защиты команд управления в инструментальной среде для автоматизированных систем управления технологическими процессами // Вестник НГУ. Серия: Информационные технологии. 2021. Т. 19, № 4. С. 5–15. DOI 10.25205/1818-7900-2021-19-4-5-15

Methods for Protecting Control Commands in the Instrumental Environment for Automated Process Control Systems

Anatoly I. Blagodarny [1], **Boris N. Pishchik** [2]

[1, 2] Federal Research Center for Information and Computing Technologies
Novosibirsk, Russian Federation

[2] Novosibirsk State University
Novosibirsk, Russian Federation

[1] ablagodarnyj@mail.ru, https://orcid.org/0000-0001-8668-1094
[2] pishchik.boris@ya.ru, https://orcid.org/0000-0001-9083-4807

Abstract

The paper discusses methods that ensure the execution of only correct and legal control commands in the process control system. Protection of the integrity of the APCS software at all nodes of the industrial network, including protec-

tion against unauthorized substitution, is carried out by checking the control parameters of the software during their startup. Protection of control commands from distortions during transmission over the network is realized by double coding at different levels of the system. Protection against the submission of unauthorized control commands to technological equipment is carried out by recognizing these commands in the lower-level subsystem and comparing their current characteristics with the control ones.

A certain contribution to the safety of the process control system is made by the use of a secure execution environment – OS CentOS 7.

Keywords

APCS, SCADA, protection methods, control commands

For citation

Blagodarnyy A. I., Pishchik B. N. Methods for Protecting Control Commands in the Instrumental Environment for Automated Process Control Systems. *Vestnik NSU. Series: Information Technologies*, 2021, vol. 19, no. 4, p. 5–15. (in Russ.) DOI 10.25205/1818-7900-2021-19-4-5-15

Введение

Для создания автоматизированных систем управления технологическими процессами (АСУ ТП), как правило, используется некоторая инструментальная среда (ИС), именуемая в различных источниках как ICS, SCADA или PLC.

Рассматриваемая в данной статье инструментальная среда является развитием и обобщением SCADA-системы «Блакарт», использованной при создании нескольких конкретных АСУ ТП, внедренных на предприятиях транспорта нефти [1; 2]. «Блакарт» имеет реализации для операционных систем реального времени «QNX 4.25» [3] и «QNX 6.5 Нейтрино» [4]. На ее основе были реализованы АСУ ТП на предприятиях угледобывающей промышленности [5–9], которые показали свои высокие эксплуатационные качества [10].

Безопасность АСУ ТП как проблема обсуждается в работах многих авторов [11–15]. Проблема многоаспектная и, безусловно, актуальная и в настоящее время.

В ФИЦ ИВТ на основе «Блакарт» ведется разработка ИС в операционной системе с открытым исходным кодом CentOS 7. Цель проекта – разработка ИС, обеспечивающей *безопасное управление* в создаваемых на их основе АСУ ТП. Не умаляя важности других проблем, в данном проекте особое внимание уделяется процессу выполнения команд управления, поскольку обеспечение корректности работы АСУ ТП в значительной степени связано с возможностью контроля исполнения команд управления с целью не допустить их несанкционированного исполнения, инициированного кибератаками, которые, в свою очередь, начинаются с поиска и использования уязвимостей как самой системы, так и среды ее исполнения.

1. Среда исполнения

Для обеспечения киберустойчивости прикладного программного обеспечения АСУ ТП инструментальная среда реализуется на операционной системе CentOS 7. Эта операционная система (ОС) выбрана как безопасная среда с открытым исходным кодом для исполнения программного обеспечения АСУ ТП. Под безопасностью здесь понимается отсутствие уязвимостей, которые могут быть использованы злоумышленником для атаки на АСУ ТП.

Исследование банка данных угроз безопасности информации ФСТЭК [1] и открытых баз данных уязвимостей NIST [2] показывает, что уязвимости в компонентах CentOS 7, необходимых для функционирования АСУ ТП (ядро системы, различные пакеты сервиса rsyslog, библиотеки OpenSSL, технологии WPA и сетевого обмена файлами (Samba)), которые могут быть использованы для удаленного доступа и исполнения кода, устранены. Эти уязвимости

[1] Банк данных угроз безопасности информации. ФСТЭК России, ФАУ «ГНИИИ ПТЗИ ФСТЭК России». URL: https://bdu.fstec.ru/.

[2] National vulnerability database. URL: https://nvd.nist.gov/.

(более 180) были обнаружены в период 2014–2015 гг., и с тех пор о новых уязвимостях в этих компонентах сообщений не было.

2. Структура инструментальной среды

Разрабатываемая ИС позволяет реализовать АСУ ТП для широкого спектра технологических процессов и состоит из двух подсистем: подсистемы верхнего уровня и подсистемы нижнего уровня. Подсистема верхнего уровня реализует функции автоматизированного рабочего места (АРМ) оператора и сервера архивных данных, подсистема нижнего уровня – доступ к контролируемому технологическому оборудованию.

Обмен данными между указанными выше подсистемами осуществляется по каналам связи локальной вычислительной сети (технологическая сеть), объединяющей только АРМы и технологическое оборудование. Сеть состоит из узлов, каждый из которых является вычислительным устройством, на котором запущена или подсистема верхнего уровня, или (и) подсистема нижнего уровня. В технологической сети особое место занимает один выделенный узел, который называется узлом системного администратора. Связь технологической сети с другими сетями предприятий осуществляется только через выделенные сетевые адаптеры шлюзового компьютера с контролем используемых сетевых сервисов, например, при помощи односторонних сетевых адаптеров.

Подсистема верхнего уровня состоит из набора программных модулей: модуль графического интерфейса оператора, модуль базы данных, модуль синхронизации времени, модуль контроля состояния технологической сети, модуль контроля текущего состояния программного обеспечения на узлах технологической сети, модуль контроля целостности программного обеспечения на узлах технологической сети, а также буферные модули обмена данными.

Подсистема нижнего уровня включает в себя набор драйверов обслуживания плат ввода / вывода, драйверов связи с логическими контроллерами и буферные модули обмена данными. Общая структура среды представлена на рисунке, где светлые линии показывают пути передачи данных от датчиков к компьютерам, а темные линии – пути передачи команд управления от компьютеров к драйверам и исполнительным механизмам. Серые линии указывают на каналы синхронизации времени в узлах.

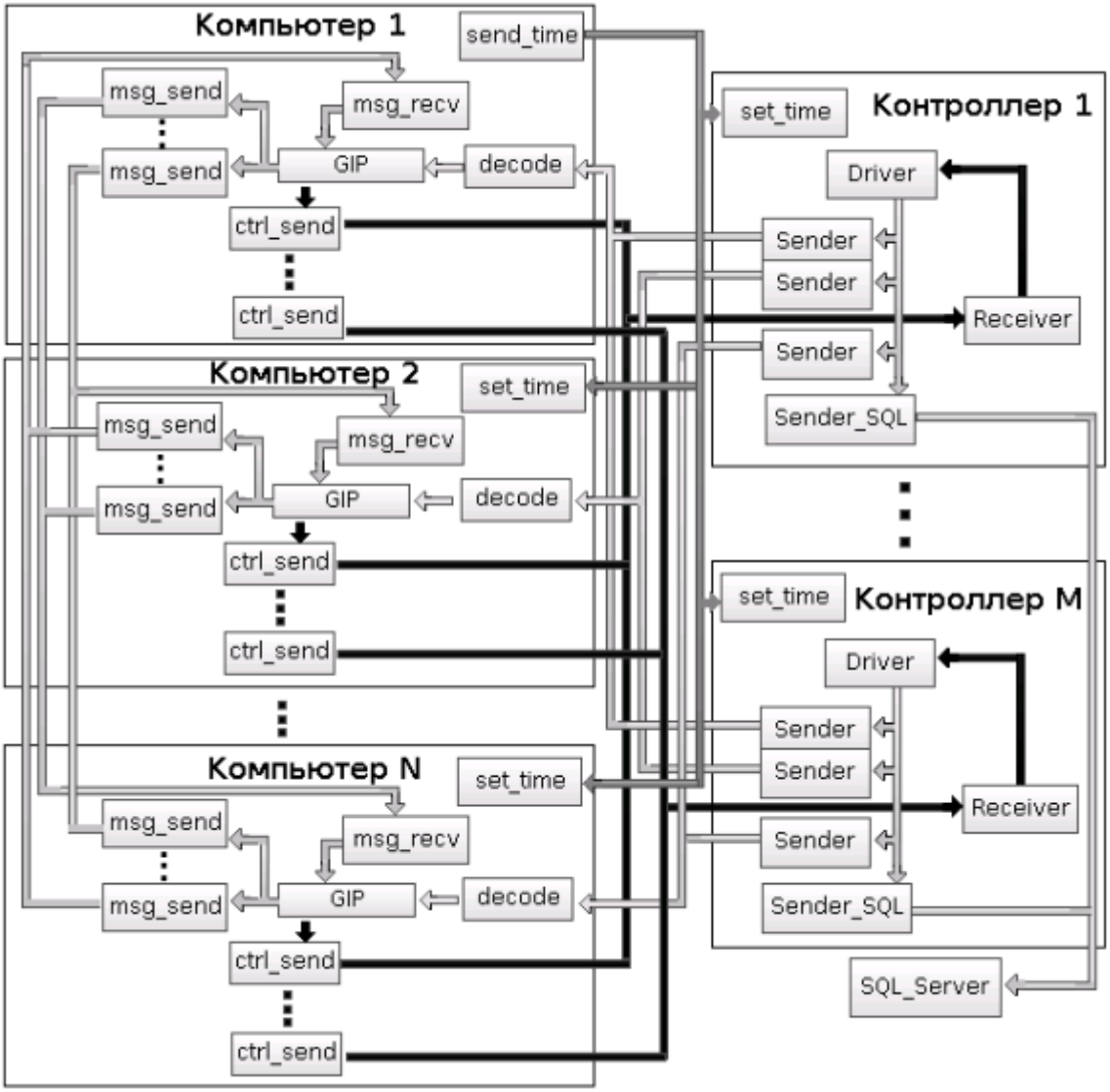
На физическом уровне в технологической сети используется канальный протокол технологии Ethernet. Обмен данными между программными модулями, находящимися на различных узлах технологической сети, осуществляется только по протоколу нижнего уровня UDP стека протоколов TCP/IP.

Основными достоинствами указанного протокола являются максимальная помехоустойчивость, максимальное быстродействие, максимально низкий сетевой трафик, а также наличие в пакетах данных всей идентифицирующей взаимодействующих абонентов информации. Для адресации абонентов в пределах технологической сети используются локальные IP-адреса.

К недостаткам протокола UDP относится необходимость подтверждения обмена данными, поскольку надежность доставки данных, а также отсутствие искажений в переданных данных не гарантируются. Впрочем, несмотря на декларируемый метод гарантированной доставки данных при использовании транспортного протокола TCP, как правило, для всего разрабатываемого прикладного программного обеспечения все равно используется или механизм подтверждения обмена данными, или контроль последовательности передаваемых пакетов данных, поскольку всегда существует возможность несанкционированного разрыва установленного соединения между взаимодействующими абонентами.

Обмен данными между программными модулями, находящимися на одном узле технологической сети, осуществляется только через *буферы данных в разделяемой оперативной памяти*. Указанные буферы памяти открываются только на чтение для всех программных

модулей, исключая владельца буфера данных (того, кто создал буфер данных). Для владельца доступны как операция чтения, так и операция записи.



Общая структура инструментальной среды
General structure of the instrumental environment

Создание конкретного проекта АСУ ТП в инструментальной среде включает в себя только разработку графического интерфейса оператора и написание текстовых конфигурационных файлов подсистемы верхнего уровня, подсистемы нижнего уровня и конфигурационного файла технологической сети (средства конфигурирования).

Конфигурационные файлы подсистемы верхнего уровня (КФВУ) определяют 17-значные символьные коды сигналов состояния и управления технологическими объектами, а также методы обработки и методы отображения сигналов, полученных от контролируемого технологического оборудования сигналов, на графическом интерфейсе оператора.

Конфигурационные файлы подсистемы нижнего уровня (КФНУ) задают кодировку сигналов состояния и управления, представляющую собой пятерку неотрицательных коротких (16-разрядных) целых чисел и определяют последовательность распределения сигналов состояния и управления по датчикам и исполнительным реле системы сопряжения с технологическим оборудованием.

Конфигурационный файл технологической сети определяет список допустимых номеров узлов технологической сети, присвоенные узлам локальные IP-адреса и прочую информацию, идентифицирующую узлы.

3. Методы защиты команд управления

Методы защиты команд управления технологическим оборудованием в АСУ ТП можно разделить на три основных направления:

- методы защиты целостности прикладного программного обеспечения;
- методы защиты команд управления от ошибок передачи данных по технологическим сетям;
- методы защиты от подачи на контролируемое технологическое оборудование несанкционированных команд управления.

3.1. Защита целостности прикладного программного обеспечения

Прикладное программное обеспечение (ППО) АСУ ТП имеется на каждом узле сети. Однако особым узлом технологической сети является узел системного администратора. На узле системного администратора хранится образцовое программное обеспечение инструментальной среды, часть модулей которого тиражируется на другие узлы и используется в конкретной АСУ ТП в качестве прикладного программного обеспечения на верхнем и нижнем уровнях. Таким образом, особого внимания требует защита узла системного администратора
от несанкционированного внешнего доступа и / или нарушения целостности программного обеспечения на нем. Здесь применяются криптографические методы аутентификации и авторизации, а также административные регламенты допуска к работе с системой.

Методы защиты целостности ППО АСУ ТП на всех узлах технологической сети включают защиту от несанкционированной подмены любого программного модуля или средств конфигурирования как в процессе их функционирования в оперативной памяти, так и при подмене соответствующих файлов на долговременном устройстве хранения.

При запуске ППО каждого узла производится контроль целостности всех файлов, содержащих соответствующие программные модули. Такой контроль осуществляется сравнением с образцовыми файлами ППО, находящимися на узле системного администратора. Метод сравнения включает в себя контроль времени и даты формирования файлов, контроль их размеров и проверку контрольных сумм программных модулей. В случае обнаружения нарушения целостности файлов ППО модуль контроля целостности прекращает запуск ППО узла и формирует аварийный сигнал с указанием номера узла и имени поврежденного программного модуля, который передается на все АРМ оператора технологической сети.

ППО ИС функционирует на узлах технологической сети в виде заданного набора процессов. Каждый процесс в каждый момент времени характеризуется своим состоянием. Из всех возможных состояний процессов аварийными состояниями (иначе называемые сбоем ППО) являются только два: состояние «убит (закрыт)» и состояние «зомби (закрыт, но информация о процессе еще существует в ядре операционной системы)». При обнаружении указанных аварийных состояний каких-либо процессов АСУ ТП программный модуль контроля состояния ППО автоматически формирует аварийный сигнал с указанием названия аварийного программного модуля, его состояния и номера узла. Далее сформированный ава-

рийный сигнал немедленно пересылается на все АРМ оператора. Таким образом, всякая попытка подмены любого программного модуля в процессе его функционирования будет немедленно замечена системой контроля.

Контроль целостности файлов средств конфигурирования при запуске ППО какого-либо узла технологической сети полностью аналогичен контролю целостности файлов программных модулей и осуществляется модулем контроля целостности ППО.

Средства конфигурирования при запуске ППО загружаются в конфигурационные таблицы в разделяемой оперативной памяти, открытой только на чтение. Поскольку доступ к конфигурационным таблицам на запись запрещен, то для подмены конфигурационных таблиц в разделяемой памяти в процессе функционирования ППО необходимо предварительно удалить ранее созданные таблицы и только затем создать новые конфигурационные таблицы. Но в результате подобной операции доступ к вновь созданным таблицам со стороны функционирующих модулей АСУ ТП будет утерян (меняется их адрес в разделяемой оперативной памяти). Это обстоятельство приводит к сбою ППО и формированию программой контроля состояния ППО соответствующих аварийных сигналов с передачей на все АРМ оператора.

3.2. Защита от ошибок передачи команд управления

Протокол нижнего уровня «UDP» контролирует только управляющую информацию в передаваемых дейтаграммах. Контроль пользовательских данных должен осуществляться программным обеспечением АСУ ТП.

Все коды сигналов управления, имеют 2 кодировки: в подсистеме верхнего уровня и в подсистеме нижнего уровня. Все эти коды перечислены в КФВУ и КФНУ.

Передача команд управления из подсистемы верхнего уровня в подсистему нижнего уровня осуществляется управляющими пакетами.

В состав управляющего пакета входят:

- поле кода сигнала управления в кодировке подсистемы верхнего уровня (17-значный символьный код суммарной длиной 136 бит) из КФВУ;
- поля кода сигнала управления в кодировке подсистемы нижнего уровня (пятерка коротких целых неотрицательных чисел суммарной длиной 80 бит) из КФНУ;
- поля авторизации (пароль и идентификатор) оператора и некоторые другие поля.

Далее управляющий пакет передается в подсистему нижнего уровня, где соответствующий драйвер принимает управляющий пакет и проверяет наличие принятого кода сигнала управления в КФВУ. Если такой сигнал существует в КФВУ, то из КФНУ извлекается соответствующий ему код. Далее принятый код сигнала управления и код сигнала из КФНУ сравниваются, и если коды совпали, то сигнал передается на исполнение.

Если сигнал управления с кодом в кодировке подсистемы верхнего уровня не существует или обнаружено расхождение в сравниваемых кодах в кодировке подсистемы нижнего уровня, то производится повторный запрос сигнала управления и далее, при повторной ошибке, драйвер формирует сигнал о невозможности управления, который передается на все АРМ оператора.

Отметим, что при таком подходе вероятность того, что *искаженный* при передаче сигнал управления окажется *допустимым*, очень мала.

Предположим, что общее число команд управления в конфигурационных таблицах равно 1000. А общее число возможных кодов сигналов управления в кодировке подсистемы верхнего уровня (общая длина кода 136 бит) равно 2^{136} или $\sim 10^{45}$. Тогда вероятность того, что искаженный при передаче сигнал управления в кодировке подсистемы верхнего уровня окажется допустимым, равна примерно $1000/10^{45}$, или числу с 42 нулям после запятой. Искаженному сигналу управления может соответствовать только один допустимый сигнал управления в кодировке подсистемы нижнего уровня (общая длина кода 80 бит). Вероятность его синхронного искажения равна $1/2^{80}$, или примерно числу с 26 нулями после запятой.

Общая вероятность незамеченного подсистемой нижнего уровня искажения при передаче сигнала управления является произведением вышеуказанных вероятностей и равна примерно числу с 68 нулям после запятой, т. е. *практически нулевой*.

3.3. Защита от подачи на контролируемое технологическое оборудование несанкционированных команд управления

3.3.1. Распознавание несанкционированных команд управления в подсистеме нижнего уровня

Структура технологической сети имеет ключевое значение для безопасного управления, определяется на этапе ее проектирования и записывается в конфигурационный файл технологической сети (КФТС). Этот файл содержит следующую информацию для каждого узла сети: номер узла, имя узла, тип подсистемы, IP-адрес, флаг базового узла.

Параметр «имя узла» содержит имя установленной операционной системы на узле с десятичным номером – «номер узла». Параметр «тип подсистемы» определяет тип подсистемы (верхний или нижний уровень), запущенной на данном узле. Параметр «флаг базового узла» определяет указанный узел как узел системного администратора с образцовым системным временем.

Если на каком-либо узле технологической сети одновременно запущены и подсистема верхнего уровня, и подсистема нижнего уровня, то такой узел указывается дважды, но с различными значениями номера узла.

Номера портов обмена данными рассчитываются в соответствии с типом подсистемы (верхний или нижний уровень) и номером узла по определенному алгоритму и являются строго фиксированными для каждого узла технологической сети.

Все команды управления технологическим оборудованием, поступающие на вход подсистемы нижнего уровня, *формируются исполняющей системой стека протоколов TCP/IP*, являются дейтаграммами в формате протокола UDP и несут в себе полную информацию о взаимодействующих абонентах, в частности IP-адреса и номера портов обмена данными. Порты обмена данными протокола UDP являются числовыми идентификаторами, однозначно определяющими программные модули, участвующие в обмене.

После получения команды управления подсистема нижнего уровня, используя КФТС, по полученному IP-адресу определяет номер узла, с которого была подана команда. Далее рассчитывается номер порта, с которого должна была быть подана команда.

Команда управления считается несанкционированной если:

- команда является неавторизованной, или код авторизации не является разрешенным системным администратором;
- полученный IP-адрес не найден в конфигурационной таблице технологической сети, или узел с указанным IP-адресом не является узлом с подсистемой верхнего уровня в той же конфигурационной таблице;
- рассчитанный номер порта не совпадает с полученным номером порта в дейтаграмме команды.

Несанкционированная команда управления игнорируется, и драйвер подсистемы нижнего уровня формирует аварийный сигнал, который передается на все АРМ оператора.

3.3.2. Защита от внедрения в дисциплину обмена несанкционированных команд управления

Возможны только два варианта внедрения в алгоритм передачи команд управления с верхнего на нижний уровень системы:

- от внешнего по отношению к технологической сети абонента;

- с помощью программного модуля, внедренного на какой-либо узел технологической сети.

В первом варианте (внедрение внешнего абонента) IP-адрес внешнего по отношению к технологической сети абонента является *посторонним*, не содержится в конфигурационном файле технологической сети, и команда, посланная внешним абонентом, будет отвергнута драйвером подсистемы нижнего уровня с передачей на все АРМ оператора сигнала о попытке постороннего вторжения.

Во втором варианте (команда от внедренного модуля) также возможны только два способа попытки внедрения в дисциплину обмена несанкционированных команд управления: запись команды в буфер команд в разделяемой оперативной памяти в подсистеме верхнего или подсистеме нижнего уровня и непосредственная передача команды в подсистему нижнего уровня.

При первом способе запись несанкционированной команды в буфер команд в разделяемой оперативной памяти будет отвергнута операционной системой, так как буфер команд создан с атрибутом только для чтения.

При втором способе IP-адрес переданной команды может быть вполне легальным, с точки зрения конфигурационного файла технологической сети. Но номера портов обмена данными определяются только номерами узлов технологической сети и жестко закреплены за всеми программными модулями ППО узлов технологической сети. Исходя из вышесказанного, номер порта переданной в подсистему нижнего уровня команды от постороннего программного модуля не будет являться легальным, и команда будет отвергнута драйвером подсистемы нижнего уровня с передачей на все АРМ оператора сигнала о попытке постороннего вторжения.

Заключение

Изложенные выше методы используются в инструментальной системе, на базе которой реализованы промышленные АСУ ТП в нефтегазовой отрасли и угольной промышленности. Отказоустойчивость и киберустойчивость этих АСУ ТП проверена многолетним опытом эксплуатации.

В настоящей статье не рассматриваются вопросы защиты системного программного обеспечения. Основное внимание уделяется защите прикладного программного обеспечения инструментальной среды в части защиты контролируемого технологического оборудования от подачи на него неверных или несанкционированных команд управления, которые несут в себе наибольшую опасность.

Однако представляется очевидным тот факт, что описанная методика защиты команд управления технологическим оборудованием вполне применима и к защите обмена самыми произвольными данными по технологическим сетям.

Список литературы

1. **Золотухин Е., Михальцов Э., Старшинов А., Стратула В., Чейдо Г.** Модернизация АСУ ТП магистральных нефтепроводов // Современные технологии автоматизации. 1997. № 4. С. 18–26.
2. **Благодарный А., Зензин А., Михальцов Э., Петков А., Чейдо Г.** Программируемая информационно-управляющая система – инструмент создания АСУ ТП магистральных нефтепроводов // IT-решения в нефтегазовой отрасли. М.: ИД «Нефть и капитал», 2002. С. 51–58.
3. **Благодарный А. И., Каратышева Л. С.** Универсальная SCADA-системы «Блакарт» под управлением операционной системы QNX // Проблемы информатики. 2009. № 3. С. 62–67.

4. **Благодарный А. И.** Программный инструментарий для построения систем автоматизированного управления в среде отечественной операционной системы // Проблемы информатики. 2018. № 2. С. 41–51.
5. **Благодарный А. И., Гаркуша В. В., Цыба А. М., Чейдо Г. П., Шевченко Д. О., Яковлев В. В.** Автоматизированное управление электроснабжением угольной шахты // Энергетическая безопасность России. Новые подходы к развитию угольной промышленности: Сб. тр. XV Междунар. науч.-практ. конф. / Под ред. В. И. Клишина, З. Р. Исмагилова, В. Ю. Блюменштейна, С. И. Протасова, Г. П. Дубинина. Кемерово: Ин-т угля СО РАН, 2013. С. 264–266.
6. **Благодарный А. И., Гаркуша В. В., Цыба А. М., Шевченко Д. О., Яковлев В. В., Чейдо Г. П.** Автоматизированная система управления наземным и подземным электроснабжением угольной шахты // Вычислительные технологии. 2013. Т. 18. С. 113–116.
7. **Благодарный А. И., Гусев О. З., Журавлев С. С., Зензин А. С., Золотухин Е. П., Каратышева Л. С.** Автоматизированная система наблюдения, оповещения и поиска персонала при авариях в шахтах // Горная промышленность. 2009. № 1. С. 34–38.
8. **Благодарный А. И., Гусев О. З., Журавлев С. С., Золотухин Е. П., Каратышева Л. С., Колодей В. В., Михальцов Э. Г., Чейдо Г. П., Шакиров Р. А., Шакиров С. Р.** Автоматизированная система контроля и управления ленточными конвейерами на угольных шахтах // Горная промышленность. 2008. № 5 (81). С. 38–44.
9. **Чейдо Г. П., Благодарный А. И., Собстель Г. М., Сабуров В. С., Шакиров С. Р.** Возможности диагностики состояния системы электроснабжения горнодобывающего предприятия по ансамблям измерений // Фундаментальные и прикладные исследования, разработка и применение высоких технологий в промышленности и экономике: Сб. ст. XIII Междунар. науч.-практ. конф. СПб., 2012. С. 309–311.
10. **Благодарный А. И.** Особенности и опыт применения надежной SCADA-системы «Блакарт // Индустриальные информационные системы: Сб. тез. докл. Всерос. конф. Новосибирск, 2013. С. 10.
11. **Голушко С. К., Пищик Б. Н.** Функциональность и безопасность АСУ ТП // Фундаментальная информатика, информационные технологии системы управления: реалии и перспективы. FIITM-2014: Материалы Междунар. науч.-практ. конф. Красноярск, 2014. С. 85–91.
12. **Воронцов А.** Автоматизированные системы управления технологическими процессами // Вопросы безопасности: Информ. бюлл. компании «Инфосистемы Джет». Информационная безопасность промышленных объектов. URL: http://www.jetinfo.ru/jetinfo_arhiv/informatsionnaya-bezopasnost-promyshlennykh-obektov/2011/?nid=77f3dbdaa8dfb77077c0888a712a3e1a
13. **Грицай Г., Тиморин А., Гольцев Ю., Ильин Р., Гордейчик С., Карпин А.** Безопасность промышленных систем в цифрах v2.1*. URL: http://www.ptsecurity.ru/ download/SCADA_analytics_russian.pdf
14. **Пищик Б. Н.** Безопасность АСУ ТП // Вычислительные технологии. 2013. Т. 18. Спец. вып. Труды Всероссийской конференции «Индустриальные информационные системы-2013».
15. **Мальнев А.** Защита АСУ ТП: от теории к практике // Информационная безопасность. 2012. № 6. С. 24–26.

References

1. **Zolotukhin E., Mikhaltsov E., Starshinov A., Stratula V., Cheido G.** Modernization of automated control systems of trunk oil pipelines. *Modern automation technologies*, 1997, no. 4, pp. 18–26. (in Russ.)

2. **Blagodarny A. I, Zenzin A., Mikhaltsov E., Petkov A., Cheido G.** A programmable information and control system is a tool for creating automated control systems for trunk oil pipelines. In: IT solutions in the oil and gas industry. Moscow, Oil and Capital Publ., 2002, pp. 51–58. (in Russ.)
3. **Blagodarny A. I., Karatysheva L. S.** Universal SCADA system "Blackart" running the QNX operating system. *Problems of Computer Science*, 2009, no. 3, pp. 62–67. (in Russ.)
4. **Blagodarny A. I.** Software tools for building automated control systems in the domestic operating system environment. *Problems of Computer Science*, 2018, no. 2, pp. 41–51. (in Russ.)
5. **Blagodarny A. I., Garkusha V. V., Tsyba A. M., Cheido G. P., Shevchenko D. O., Yakovlev V. V.** Automated control of coal mine power supply. In: Energy Security of Russia. New approaches to the development of the coal industry. Proc. of the XV International Scientific and Practical Conference. Eds. V. I. Klishin, Z. R. Ismagilov, V. Yu. Blumenstein, S. I. Protasov, G. P. Dubinin. Kemerovo: Institute of Coal SB RAS, 2013, pp. 264–266. (in Russ.)
6. **Blagodarny A. I., Garkusha V. V., Tsyba A. M., Shevchenko D. O., Yakovlev V. V., Cheido G. P.** Automated control system for ground and underground power supply of a coal mine. *Computing Technologies*, 2013, vol. 18, pp. 113–116. (in Russ.)
7. **Blagodarny A. I., Gusev O. Z., Zhuravlev S. S., Zenzin A. S., Zolotukhin E. P., Karatysheva L. S.** Automated system of monitoring, notification and personnel search in case of accidents in mines. *Mining Industry*, 2009, no. 1, pp. 34–38. (in Russ.)
8. **Blagodarny A. I., Gusev O. Z., Zhuravlev S. S., Zolotukhin E. P., Karatysheva L. S., Kolodey V. V., Mikhaltsov E. G., Cheido G. P., Shakirov R. A., Shakirov S. R.** Automated control system for belt conveyors at coal mines. *Mining Industry*, 2008, no. 5 (81), pp. 38–44. (in Russ.)
9. **Cheido G. P., Blagodarny A. I., Sobstel G. M., Saburov V. S., Shakirov S. R.** Possibilities of diagnostics of the state of the power supply system of a mining enterprise by ensembles of measurements. In: Fundamental and applied research, development and application of high technologies in industry and economics. Collection of articles of the XIII International Scientific and Practical Conference. St. Petersburg, 2012, pp. 309–311. (in Russ.)
10. **Blagodarny A. I.** Features and experience of using a reliable SCADA system “Blackart”. In: Industrial Information Systems. Collection of abstracts. Novosibirsk, 2013, p. 10. (in Russ.)
11. **Golushko S. K., Pishchik B. N.** Functionality and safety process control system. In: Fundamental science, information technology management system: realities and prospects. FIITM-2014. Proc. of the International scientific-practical conference. Krasnoyarsk, SFU Press, 2014, pp. 85–91. (in Russ.)
12. **Vorontsov A.** Automated process control systems. In: Safety issues. Information bulletin of the company “Jet Infosystems”. Information security of industrial facilities. (in Russ.) URL: http://www.jetinfo.ru/jetinfo_arhiv/informatsionnaya-bezopasnost-promyshlennykh-obektov/ 2011 /?nid=77f3dbdaa8dfb77077c0888a712a3e1a
13. **Gritsai G., Timorin A., Goltsev Yu., Ilyin R., Gordeychik S., Karpin A.** Safety of industrial systems in numbers v2.1*. (in Russ.) URL: http://www.ptsecurity.ru/download/SCADA_ analytics_russian.pdf
14. **Pishchik B. N.** Safety of the automated control system. *Computing Technologies*, 2013, vol. 18. Special issue: Proc. of the All-Russian Conference “Industrial Information Systems-2013”. (in Russ.)
15. **Malnev A.** Protection of automated control systems: from theory to practice. *Information Security*, 2012, no. 6, pp. 24–26. (in Russ.)

Информация об авторах

Анатолий Иванович Благодарный, научный сотрудник
Борис Николаевич Пищик, кандидат технических наук, старший научный сотрудник, доцент
SPIN 4297-3046
Author ID 13080

Information about the Authors

Anatoly I. Blagodarny, Researcher
Boris N. Pishchik, Candidate of Technical Sciences, Senior Researcher, Associate Professor
SPIN 4297-3046
Author ID 13080

Статья поступила в редакцию 11.09.2021;
одобрена после рецензирования 01.12.2021; *принята к публикации 01.12.2021*
The article was submitted 11.09.2021;
approved after reviewing 01.12.2021; *accepted for publication 01.12.2021*