УДК 004.3; 004.4

ПРОГРАММНО-ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

[1]Ф.Г. Пашаев, [2]Д.И. Зейналов, [3]Г.Т. Наджафов

[1]Министерство науки и образования Азербайджанской Республики, Институт систем управления, Баку, Азербайджан

[2]Нахчыванский государственный университет, Нахчыван, Азербайджан,

[3]Университет «Нахчыван», Нахчыван, Азербайджан

Аннотация. Быстрое развитие технологических компьютерных сетей и систем SCADA неизбежно ускорило процесс интеграции между этими сетями и глобальными сетями Интернета. В результате решение многих задач технологических и производственных процессов было упрощено, созданы возможности для удаленного управления персоналом предприятия и оперативным персоналом. Однако эта ситуация создала новые, ранее не существующие, угрозы для систем мониторинга, диагностики и управления. Различные специализированные группы, хакеры и иногда правительственные учреждения

проводят целенаправленные атаки на определенные промышленные предприятия через Интернет. Разработанный набор технических средств основан на применении контроллеров типа STM32F4XX и LPT-портов компьютеров. Информационный обмен между двумя сетями осуществляется с помощью нестандартного протокола с использованием контроллера STM32F4XX и LPT-порта.
Ключевые слова: кибератаки, технологические компьютерные сети, телемеханические системы, вредоносное программное обеспечение. случайные атаки. контроллер STM32F4XX, LPT-порт

SOFTWARE TECHNICAL TOOLS TO PROTECT INFORMATION

[1]F. H. Pashayev, [2]J. I. Zeynalov, [3]H. T. Najafov
[1]Ministry of Science and Education of the Republic of Azerbaijan, Institute of Management Systems, Baku, Azerbaijan
[2]Nakhchivan State University, Nakhchivan, Azerbaijan,
[3]Nakhchivan University, Nakhchivan, Azerbaijan

Abstract. It is known that the rapid development of technological computer networks and SCADA systems has necessarily accelerated the process of integration between these networks and global Internet networks. However. this situation has also created new threats previously non-existent to the above-mentioned monitoring, diagnostic and management systems. Developed set of technical means is based on the application of STM32F4XX type controllers and LPT ports of computers. These technical means and the exchange protocols created can act as a bridge between the global Internet and technological corporate computer networks. The developed software acts as a filter bridge between the global Internet and TKKŞ. Data exchange between these two networks is carried out by creating non-standard protocols using STM32F4XX controllers and LPT ports.
Keywords: Internet attacks. technological computer networks. telemechanical systems, malware, random attacks, STM32F4XX controller. LPT port

Введение

В современном мире стремительно развиваются промышленные сети, называемые технологическими компьютерными сетями (ТКС). В результате развития эти системы не могут работать без интеграции с корпоративными сетями.

Несколько десятилетий назад ТКС и сети SCADA не имели физической связи с локальными и глобальными сетями Интернет либо эта связь была очень слабой. Поэтому некоторые угрозы, исходящие от связи с Интернетом, не могли затронуть эти сети либо для их защиты было достаточно некоторых административных мер. В современном стадии разеития возрастают и риски, связанные с киберугрозами, главным образом из Интернета [1, 2].

Кибератаки могут иметь различные мотивы и во многих случаях могут осуществляться высокопрофессиональными и научно подготовленными группами, финансируемыми и поощряемыми государственными структурами.

Целью данной статьи является создание нестандартного программно-технического моста между ТКС и глобальной сетью Интернет.

Решение задачи

Строящийся мост основан на простой схеме. Мостовой компьютер Интернета обеспечивает нестандартную связь с Интернетом, с одной стороны, и с контроллером STM32F4XX с другой. На этот компьютер поступает из Интернета информация, связанная с системой управления технологическим процессом. Для передачи в систему управления технологическим процессом информация подготавливается и передается по нестандартному протоколу.

Контроллер STM32F4XX широко используется для обеспечения связи различных систем управления с технологическими процессами и техническими объектами [3, 4].

Эти контроллеры имеют много входных и выходных сигналов.

К контроллеру может быть подключено любое устройство, поддерживающее Inter-Integrated Circuit (I2C) протокол [5]. Имеется Входы и выходы для обмена с устройствами, которые могли взаимодействовать по протоколу UART (RS485).

Система состоит из двух мостовых компьютеров. Для связи с ними использовались LPT-порты с контроллерами STM32F4XX, и был разработан двусторонний протокол через LPT-порт на каждом компьютере [6]. Для этих целей используются регистр данных порта (реестр D), регистр состояния порта (реестр S), регистр управления портом (реестр C). Чтобы установить связь между этим портом и контроллерами SM32F4XX, достаточно выделить 10 двусторонних двоичных входных и выходных GPIO-контактов для LPT-порта каждого компьютера. Восемь из десяти контактов могут использоваться для записи или чтения данных, а два – для синхронизации обмена.

Используя эти технические средства, можно создать быстрый протокол моста. Для инициализации запуска протокола I2C. Для остановки протокола I2C, Для передачи и приема байтовпо протоколу I2C разработаны специальные алгоритмы.

Заключение

Разработанное программное обеспечение выполняет роль фильтрующего моста между глобальной сетью Интернет и технологическими корпоративными сетями. Обмен данными между ними осуществляется путем создания нестандартных протоколов с использованием контроллеров STM32F4XX и LPT-портов.

Полученные результаты могут использоваться для решения задач защиты телемеханических комплексов, ТКС, SCADA-систем от кибератак.

Список использованных источников

1. Чертков А. Кибербезопасность промышленной автоматизации // Control Engineering Россия. 2017. № 2(68). С. 22–25.

2. Schneider Electric // Защита систем от кибератак. 2011. Вып. 36. С. 110.

3. RM0090. Reference manual. URL: https://www.st.com/content/ccc/resource/technical/document/reference_manual/3d/6d/5a/66/b4/99/40/d4/DM00031020.pdf/files/DM00031020.pdf/jcr:content/translations/en.DM00031020.pdf (дата обращения: 04.03.2024).

4. STM32Cube. URL: https://istarik.ru/file/STM32Cube-Presentation.pdf

5. Basics of UART Communication. URL: https://web.stanford.edu/class/cs140e/notes/lec4/uart-basics.pdf (дата обращени: 04.03.2024).

6. Interfacing the Standard Parallel Port. URL: http://retired.beyondlogic.org/spp/parallel.pdf.

References

1. Chertkov A. Kiberbezopasnost promyshlennoj avtomatizacii [Cyber security of industrial automation]. *Control Engineering Rossiya* [*Control Engineering Russia*]. 2017. No. 2(68), pp. 22–25.

2. Schneider Electric [Schneider Electric]. *Zashhita sistem ot kiberatak* [*Protecting systems from cyberattacks*]. 2011. Iss. 36. p. 110.

3. RM0090. Reference manual. URL: https://www.st.com/content/ccc/resource/technical/document/reference_manual/3d/6d/5a/66/b4/99/40/d4/DM00031020.pdf/files/DM00031020.pdf/jcr:content/translations/en.DM00031020.pdf (accessed: 04.03.2024).

4. STM32Cube. URL: https://istarik.ru/file/STM32Cube-Presentation.pdf (accessed: 04.03.2024).

5. Basics of the SPI communication protocol. URL: http://www.circuitbasics.com/basics-of-the-spi-communication-protocol/ (accessed: 04.03.2024).

6. Interfacing the Standard Parallel Port. URL: http://retired.beyondlogic.org/spp/parallel.pdf.

Сведения об авторах

Пашаев Ф.Г., д-р техн. наук, доцент, Министерство науки и образования Азербайджанской Республики. E-mail: pasha.farhad@gmail.com.
Зейналов Д.И., д-р матем. наук, Нахчыванский государственный университет.
Наджафов Г.Т., старший преподаватель, Университет «Нахчыван».

Information about the authors

Pashayev F.H., Doctor of Engineering Sciences, Associate Professor, The Ministry of Science and Education of the Republic of Azerbaijan. Institute of Control Systems E-mail: pasha.farhad@gmail.com.
Zeynalov J.I., Doctor of Mathematics, Nakhchivan State Universty.
Najafov H.T., Senior Lecturer, "Nakhchivan" University.