УДК 621.3:004.7

С.Г. Семенов[1], В.В. Давыдов[1], Я.В. Илюшко[2]

[1] *Национальный технический университет «ХПИ», Харьков*
[2] *Национальный аэрокосмический университет «ХАИ», Харьков*

УЯЗВИМОСТИ ОПЕРАЦИОННОЙ СИСТЕМЫ QNX В СТРУКТУРЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ

Исследована структура автоматизированной системы управления технологическим процессом, определена одна из подсистем, наиболее подверженная программным угрозам, и возможные источники программных угроз. Проведен анализ состояния защищенности операционной системы QNX и выявлены возможные ее уязвимости в структуре АСУ технологическим процессом. Разработана схема обобщенного алгоритма возможного поведения злоумышленного программного обеспечения при атаке рассматриваемой операционной системы.

Ключевые слова: *автоматизированная система управления технологическим процессом, программная угроза, операционная система QNX.*

Введение

В соответствии с законом Украины "Про захист інформації в автоматизованих системах", государственными и международными стандартами [1, 5] одним из факторов, влияющих на эффективность функционирования любой автоматизированной системы управления (АСУ), является состояние защиты ее

ее программных и аппаратных средств. В этой связи в настоящее время при разработке и внедрении средств АСУ рассматривается ряд подходов, направленных на обеспечение требуемых показателей безопасности. Одним из таких подходов является внедрение защищенной операционной системы (ОС).

Проведенный анализ ОС реального времени показал, что среди подобных систем наиболее защищенными являются UNIX-системы.

В силу ряда преимуществ структурного и технического характеров (работа в режиме реального времени, технология микроядра, модульная архитектура, соответствие стандарту POSIX, многозадачность, неограниченные сетевые возможности, заложенные на уровне ядра, компактность, обилие развитых средств разработки и др.) разработчики в последнее время все чаще выделяют ОС QNX. Однако, как показали исследования, данная операционная система не лишена недостатков. Среди них следует выделить полное отсутствие средств выявления, идентификации и локализации программных угроз безопасности (компьютерных вирусов). Особую актуальность данная проблема приобретает в автоматизированных системах управления технологическим процессом (АСУ ТП), поскольку даже небольшой сбой в их функционировании может привести к существенным негативным последствиям.

Анализ литературы [2 – 6] и ряда научных статей [7, 8] показал, что разработчики специализированного программного обеспечения недостаточно внимания уделяют внедрению средств антивирусной защиты в ОС QNX, мотивируя это чаще всего небольшой вероятностью вирусных атак. Однако, как показали исследования, в связи с все большим распространением и расширением пользовательской аудитории ОС QNX вероятность проведения на них вирусных атак увеличивается. Поэтому анализ состояния защищенности ОС QNX и выявление возможных ее уязвимостей в структуре АСУ ТП является актуальной научной задачей. Рассмотрим структуру и основные элементы АСУ ТП.

Основной материал исследований

1. Исследование структуры и процесса взаимодействия внутренних систем АСУ ТП.

На рис. 1 представлена структурно-функциональная схема АСУ ТП. Как видно из рисунка, АСУ ТП состоит из нескольких внутренних систем и инфраструктуры телекоммуникаций.

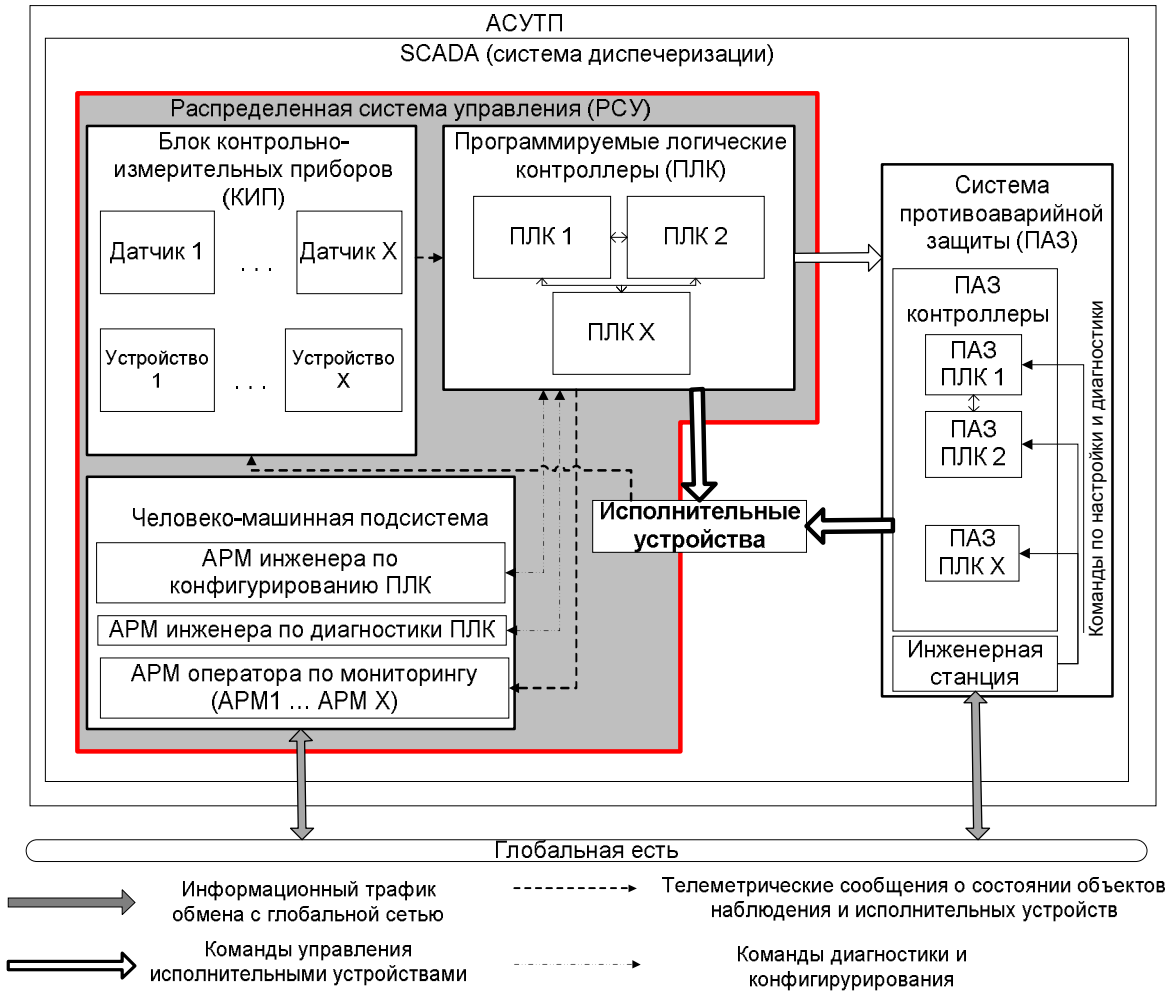

Рис. 1. Структурно-функциональная схема АСУ ТП

Проведенный анализ структуры АСУ ТП показал, что для обеспечения безопасности информационного обмена и сигнализации о нарушениях функционирования в рассматриваемой системе используются процедуры, заложенные в алгоритм взаимодействия распределенной системы управления (РСУ) с системой противоаварийной защиты (ПАЗ).

Как видно из рис. 1, основное участие в процессе взаимодействия РСУ и ПАЗ принимают блоки контрольно-измерительных приборов, программируемых логических контроллеров (ПЛК) и блок ПАЗ контроллеров, при этом команды мониторинга, диагностики и управления на указанные блоки поступают от автоматизированных рабочих мест (АРМ) человеко-машинной системы.

Проведенные исследования показали, что одним из основных источников программных угроз АСУ ТП является человеко-машинная подсистема. Связано это в первую очередь с тем, что именно эта подсистема имеет точки входа и выхода во внешние локальные и глобальные телекоммуникационные сети и, следовательно, именной эта подсистема может быть подвержена внешним программным угрозам.

2. Анализ уязвимостей ОС QNX.

На рис. 2 представлена схема обобщенного алгоритма возможного поведения злоумышленного программного обеспечения (компьютерного вируса) при атаке ОС QNX АСУ ТП. Как видно из рисунка, первой задачей компьютерного вируса является проникновение в АСУ ТП. На данной стадии вирус может проникать в систему с внешних переносных накопителей или через незащищенную внешнюю сеть с последующим заражением АРМ человеко-машинной подсистемы. Для выполнения злонамеренных задач компьютерный вирус на каждом АРМ должен получить привилегированные права, при этом он может воспользоваться уязвимостями ОС.

Анализ ОС QNX показал ряд уязвимостей алгоритма получения прав «суперпользователя». Это в частности:

– уязвимости в phgrafx при указании длинного имени .pal файла в папке *palette/*;

– уязвимость, связанная с тем, что в QNX файл */etc/rc.d/rc.local* поставляется с правами записи для всех пользователей (данная уязвимость предполагает, что хост – не ПЛК, так как для своего функционирования предполагает перезагрузку системы). Содержимое файла */etc/rc.d/rc.local* выполняется с правами администратора при загрузке системы;

– уязвимость, основанная на вводе длинных (более 255 символов) аргументов команд *su* и *passwd* (команда *su* предназначена для перехода в режим «суперпользователя» команда *passwd* предназначена для смены пароля текущего пользователя);

– уязвимость в команде *phfont* при манипулировании значениями переменных окружения PHFONT и PHOTON2_PATH;

– уязвимость, связанная с заданием длинного значения параметра «-s» для следующих команд: *phrelay-cfg, phlocale, pkg-installer, input-cfg;*

– уязвимости связанные с заданием специальной последовательности операторов для приложения gdb. GDB (GBU Debugger), которое поставляется с gcc компилятором:

*echo -e "break *0xb032d59\f\n\r\n\cont\n\cont" | gdb gdb;*

– уязвимость, связанная с записью в память определенной последовательности команд:

xor eax, eax
push eax
push $0x68732f2f
push $0x6e69622f
push esp
mov $0xDEADBEEF, ebx.

Рис. 2. Схема обобщенного алгоритма возможного поведения злоумышленного программного обеспечения (компьютерного вируса) при атаке ОС QNX АСУ ТП

Как видно из рис. 2, если компьютерный вирус не получил права «суперпользователя» – он заканчивает свою работу в связи с тем, что у него не будет необходимых привилегий выполнения специфических команд.

В случае получения привилегированных прав, в зависимости от реализации и намерений злоумышленника, вирус может выполнять следующие действия:

1. Сбор данных. На данном этапе в течении определенного времени вирус собирает информацию о командах, поступающих на ПЛК, а так же данные, посылаемые на АРМ с заданной злоумышленником периодичностью. Данная информация передается через глобальную сеть злоумышленнику. В зависимости от ответа злоумышленника, вирус может продолжать собирать информацию. Для передачи данных злоумышленнику вирусу необходимо:

– доступ в глобальную сеть;

– наличие открытых портов, через которые можно передавать данные.

2. В качестве ответа злоумышленника на переданные данные должен прийти ответ о необходимости продолжения сбора данных.

3. Ожидание «особого» времени. Данное «особое» время задается злоумышленником. Одной из причиной данного действия является избежание преждевременного обнаружения злоумышленного программного обеспечения или одновременная атака зараженных машин с целью полной деактивации производственного процесса.

4. Выполнение деструктивных действий (вирус выполняет цепочку функций, заданных злоумышленником).

Выводы

Таким образом, проведенные исследования показали необходимость обнаружения и локализации программных угроз АСУ ТП с операционной системой QNX. В результате работы проведен анализ алгоритма возможного поведения злоумышленного программного обеспечения (компьютерного вируса) при атаке ОС QNX АСУ ТП, а также выявлены уязвимости данной операционной системы. В дальнейшем это может дать возможность разработать математическую модель компьютерного вируса среде ОС QNX и создать систему идентификации программных угроз АСУ ТП с операционной системой QNX.

Список литературы

1. Закон України «Про внесення змін до Закону України "Про захист інформації в автоматизованих системах" (Відомості Верховної Ради України (ВВР), 2005, N 26, ст.347).

2. Горошко Е. QNX/UNIX: анатомия параллелизма / Е. Горошко, О. Цилюрик. – М.: Символ-Плюс,·2006. – 288 с.

3. Денисенко В.В. Компьютерное управление технологическим процессом, экспериментом, оборудованием / В.В. Денисенко. – М.: Горячая линия–Телеком, 2009. – 608 с.

4. Кртен Р. Введение в QNX Neutrino. Руководство для разработчиков приложений реального времени (2-е издание) / Р. Кртен. – СПб.: БХВ-Петербург, 2011. – 368 с.

5. Кузнецов О.О. Протоколи захисту інформації у комп'ютерних системах та мережах: навч. посібник / О.О. Кузнецов, С.Г. Семенов. – Х.: ХНУРЕ, 2009. – 186 с.

6. *Операционная система реального времени QNX Neutrino 6.3. Руководство пользователя / перевод Ю. Асотов. – СПб.: БХВ-Петербург, 2009. – 480 с.*

7. Семенов С.Г. Безопасность операционных систем реального времени в автоматизированных системах управления технологическим процессом / С.Г. Семенов, С.Ю. Гавриленко, В.В. Давыдов // Авиационно-космическая техника и технология. – 2011. – № 8(85). – С. 222-225.

8. Tanenbaum Andrew S. Can We Make Operating Systems Reliable and Secure? / Andrew S. Tanenbaum, Jorrit Herder, Herbert Bos // Vrije Universiteit, Amsterdam. Computer (IEEE Computer Society, V. 39, No 5, May 2006).

Поступила в редколлегию 26.01.2012

Рецензент: канд. физ.-мат. наук, ст. научн. сотр. А.А. Можаев, Национальный технический университет «ХПИ», Харьков.

УРАЗЛИВОСТІ ОПЕРАЦІЙНОЇ СИСТЕМИ QNX В СТРУКТУРІ АВТОМАТИЗОВАНОЇ СИСТЕМИ УПРАВЛІННЯ ТЕХНОЛОГІЧНИМ ПРОЦЕСОМ

С.Г. Семенов, В.В. Давидов, Я.В. Ілюшко

Досліджена структура автоматизованої системи управління технологічним процесом, визначена одна з підсистем, найбільш підвладна програмним погрозам, і можливі джерела програмних погроз. Проведений аналіз стану захищеності операційної системи QNX і виявлені можливі її уразливості в структурі автоматизованої системи управління технологічним процесом. Розроблена схема узагальненого алгоритму можливої поведінки зловмисного програмного забезпечення при атаці даної операційної системи.

Ключові слова: *автоматизована система управління технологічним процесом, програмна загроза, операційна система QNX.*

TO VULNERABILITY OF OPERATING SYSTEM QNX IN STRUCTURE OF AUTOMATED CONTROL THE SYSTEM BY TECHNOLOGICAL PROCESS

S.G. Semenov, V.V. Davydov, Ya.V. Ilyushko

The structure of automated control the system by a technological process is investigational, one of subsystems is certain, most subject to the programmatic threats, and possible sources of programmatic threats. The analysis of the state of protected of the operating system of QNX is conducted and the possible are exposed its vulnerability in the structure of automated control the system by a technological process. The chart of the generalized algorithm of possible conduct of ill-intentioned software is developed at the attack of the examined operating system.

Keywords: *automated control the system by a technological process, programmatic threat, operating system of QNX.*