УДК 519.688

СПЕЦИАЛИЗИРОВАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ ПРОВЕРКИ КОМПОНЕНТОВ ИНТЕГРИРОВАННЫХ СИСТЕМ БЕЗОПАСНОСТИ АЭС РАЗЛИЧНЫХ ПРОИЗВОДИТЕЛЕЙ НА ВОЗМОЖНОСТЬ ИНТЕГРАЦИИ

Д.Ю. Безуглов, М.А. Трофимов

ООО «АТЭКС». 249038, Обнинск, Калужской обл., ул. Любого, д.11, пом. 149.
Обнинский институт атомной энергетики НИЯУ МИФИ
249040, Обнинск, Калужской обл., Студгородок, 1

Физическую защиту АЭС обеспечивают интегрированные системы безопасности. Часто интеграция сводится к конкретным разработанным решениям по взаимодействию между продуктами одного разработчика. Для решения проблемы совместимости изделий различных производителей был введен отраслевой стандарт СТО 1.1.1.04.007.0814-2009 в 2009 г. Соответствие этому стандарту подтверждается аттестацией. При выполнении работ по аттестации был разработан автоматизированный стенд и специализированное программное обеспечение «AtomTest». Представлены основополагающие функции разработанного ПО, описаны механизм его работы и выходные данные. ПО «AtomTest» было применено при лабораторных испытаниях семи основных отечественных производителей ИСБ. По результатам выполненных работ шесть производителей получили аттестаты о соответствии стандарту.

Ключевые слова: физическая защита, интегрированная система безопасности, отраслевой стандарт, автоматизированный стенд, сетевой трафик, унифицированные протоколы, автомат состояний, специализированное ПО.

Физическая защита АЭС регламентирована требованиями законодательства РФ. В ее основе вне зависимости от объекта применения лежат автоматизированные системы безопасности, жизнеобеспечения и управления инженерным оборудованием. Многие разработчики называют свои «детища» интегрированными системами безопасности (ИСБ).

ИСБ представляют собой комплекс взаимодействующих программных и технических средств, предназначенных для обеспечения физической безопасности, автоматизации управления жизнеобеспечением и функционированием объекта, *обладающих технической, информационной, программной и эксплуатационной совместимостью*.

Безопасность объекта, как правило, обеспечивается несколькими подсистемами: охранной и пожарной сигнализации, контроля и управления доступом и системой телеНаблюдения, причем, разработчик этих подсистем не всегда один [1]. В этот «класси-

ческий» набор также могут входить система активного пожаротушения и инженерно-технические подсистемы обеспечения жизнедеятельности здания. Каждая из этих подсистем в отдельности отвечает за свой участок работы в соответствии с решаемыми задачами, заложенными в нее на этапе проектирования [2, 3]. К сожалению, вследствие их узкой направленности могут возникать противоречия при решении конкретных ситуаций на объекте, приводящие к серьезным проблемам:

– потере эффективности и оперативности действий службы безопасности, перегруженной большим количеством «разнокалиберных» управляющих терминалов;

– усложнению специализированных устройств управления в связи с появлением новых функций;

– несогласованности в работе различных подсистем;

– возможной выдаче подсистемами взаимоисключающих команд.

Таким образом, проблема объединения компонентов ИСБ различных производителей в единый комплекс до сих пор является актуальной [3]. Полноценное решение данной проблемы возможно только при условии функционирования систем в едином информационном пространстве с использованием унифицированного протокола обмена, регламентированного стандартом [4, 5]. В отрасли атомной энергетики таким стандартом является СТО 1.1.1.04.007.0814-2009 «Система сбора и обработки информации комплекса инженерно-технических систем физической защиты атомных станций. Технические требования» (далее Стандарт).

Данный Стандарт устанавливает единые требования к архитектуре применяемых на АЭС ИСБ, их минимальному функционалу и, что является наиболее важным, построению обмена данными между программными компонентами систем (СПО АПИ и СПО сервера) по унифицированному протоколу верхнего уровня, который представляет собой описание возможных команд, циркулирующих в ИСБ, на языке XML [6, 7].

В целях оценки соответствия типовых ИСБ Стандарту возникла необходимость проведения процедуры аттестации, по результатам которой предусмотрена выдача разработчику аттестатов о соответствии.

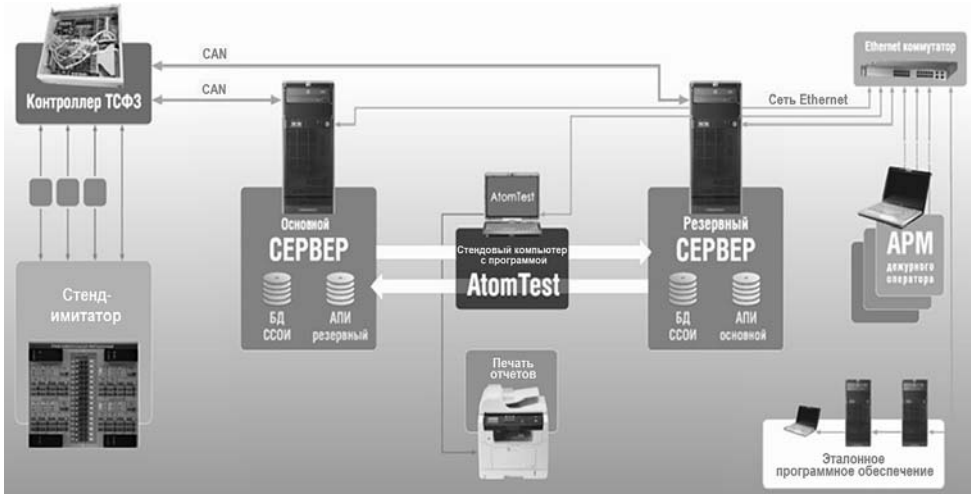

Рис. 1. Структурная схема автоматизированного стенда при выполнении проверок

Для проведения работ по аттестации в испытательной лаборатории ООО «АТЭКС» был разработан автоматизированный стенд, позволяющий испытывать полнофункциональные макеты ИСБ (рис. 1). Основополагающая функция детального анализа сетевого трафика между компонентами системы стенда возложена на специализированное программное обеспечение (СПО).

Исходя из требований Стандарта при выполнении проверок СПО должно обеспечивать решение следующих задач:

– ввод информации об испытываемых компонентах системы;

– задание параметров и глубины испытаний;

– системная перенастройка маршрутов следования пакетов данных между испытываемыми компонентами и ретрансляция сообщений;

– автоматизированное выполнение тестов испытания, включая автоматическую проверку команд, их последовательности и алгоритмов генерации на соответствие требованиям Стандарта;

– автоматический сбор и протоколирование информации о выполняемых проверках в процессе испытаний;

– ввод дополнительной информации и замечаний оператора по каждому тесту;

– протоколирование всех этапов испытаний, архивирование результатов испытаний в локальной базе данных, генерация отчетов о тестировании с последующей печатью.

Поскольку существующее ПО, позволяющее анализировать трафик компьютерных сетей (такое как Wireshark, Tcpdump), не давало возможности выполнить поставленные выше задачи, было разработано СПО «AtomTest» (далее Программа).

Программа состоит из нескольких взаимосвязанных диалоговых форм, вызываемых предопределенными алгоритмами цепочек вызовов. Диалоговые формы построены на основе web-интерфейса. Выводимая на диалоговые формы информация зависит от контекста выполнения программы.

Выполняемые испытания могут состоять из различного набора тестов. Все тесты разделены на две группы – автоматические и с участием оператора.

Для осуществления автоматической ретрансляции сообщений между компьютерным оборудованием системы используется возможность сетевых служб операционной системы пересылать все пакеты по заданным таблицам маршрутов. Программа при подключении к испытываемому комплексу выполняет изменение таблиц маршрутизации пакетов. Для этого при настройке подключений необходимо задать следующие параметры компьютерного оборудования: IP-адреса, логины и пароли пользователей, номера TCP- и UDP-портов компьютерного оборудования, через которые осуществляется обмен сообщениями.

После завершения конфигурирования Программа переходит к ожиданию инициирования обмена СПО сервера с СПО АПИ. После подключения СПО сервера к СПО АПИ производится автоматический переход к выполнению тестов.

На этапе выполнения каждого из тестов Программа, реализуя детерминированный автомат конечных состояний, ожидает заданных условий перехода от состояния к состоянию до тех пор, пока не будет достигнуто последнее состояние. Для каждого типа теста имеется свой автомат состояний, выбор автомата состояния осуществляется выбором типа теста в шаблоне описания теста. При выполнении теста Программа проверяет все команды протокола, посылаемые СПО сервера и СПО АПИ, ведет протокол всех событий. Собранная информация о выполнении теста сохраняется в папке проекта испытания и используется при формировании отчета о результатах теста с вынесением заключения о соответствии объектов испытаний. Заключение о соответствии принимается Программой автоматически на основе заданного шаблоном теста, полностью соответствующего методике данного теста, а методика в свою очередь соответствует требованиям Стандарта.

По окончании теста (по достижении последнего состояния конечного автомата состояний) Программа переходит к этапу его завершения. На форме статуса теста отображается информация о результате прохождения теста. Осуществление Про-

граммой перехода к выполнению следующего теста происходит при нажатии оператором кнопки «Продолжить» (рис. 2).

Рис.2. Форма статуса теста

По завершении заключительного теста программы испытания Программа автоматически производит обратное конфигурирование комплекса в штатный режим работы.

На следующем этапе Программа автоматически генерирует отчеты по каждому тесту испытания в форматах .html и .pdf. Длительность генерации отчетов зависит от количества тестов и объемов отчетов.

С помощью разработанной Программы были выполнены лабораторные испытания семи основных отечественных производителей ИСБ, оборудование и программное обеспечение которых поставляется на АЭС (поскольку статья не является рекламной, наименования фирм-производителей и их систем не разглашаются). Шесть производителей получили аттестаты о соответствии Стандарту.

Таким образом, полученные результаты свидетельствуют о возможности интеграции компонентов ИСБ различных производителей. Однако в ходе испытаний в тексте Стандарта были выявлены неточности и пункты, для которых возможна неоднозначная интерпретация. Несомненно, в данном направлении необходимо дальнейшее проведение работ, в том числе анализ технических решений и нормативной документации в смежных отраслях, внесение уточняющих поправок в требования Стандарта и протокола.

Литература

1.*Севрюков Д.В., Асфандияров А.Х.* Безопасность ядерных и радиационных объектов // Безопасность окружающей среды. – 2007. – №3. – С. 12-18.

2. *Звежинский С.* Проблема выбора периметровых средств обнаружения. Часть 1. // Безопасность. Достоверность. Информация. – 2002. – № 4 (44).

3. *Гарсиа М.* Проектирование и оценка систем физической защиты. – М.: Мир, ООО «Издательство АСТ», 2003 . – 386 с.

4. *Магауенов Р.Г.* Системы охранной сигнализации: основы теории и принципы построения. – М.: «Горячая линия - Телеком». – 2004. – 367 с.

5. Стандарт ОАО «Концерн Росэнергоатом» СТО 1.1.1.04.007.0814-2009 «Система сбора и обработки информации комплекса инженерно-технических систем физической защиты атомных станций». Технические требования. Введен в действие приказом ОАО «Концерн Росэнергоатом» № 1782 от 17.12.2009.

6. *Омельянчук А.М.* Стандарты на интегрированные системы безопасности – взгляд разработчика. Часть 2. // Системы безопасности. – 2006. – № 1. – С.116-120.
http://www.secuteck.ru/articles2/kompleks_sys_sec/standarty_na_integrirovannye_sist/

7. *Крахмалев А.К.* Еще раз об интеграции систем безопасности // Sec.Ru. от 26.05.2014 г.
http://daily.sec.ru/2014/05/26/Eshe-raz-ob-integratsii-sistem-bezopasnosti.html

Поступила в редакцию 26.01.2015 г.

Авторы

Безуглов Дмитрий Юрьевич, специалист ООО «АТЭКС», аспирант
E-mail: d1.bezuglov@gmail.com

Трофимов Максим Адольфович, профессор, доктор техн. наук
E-mail: trofimovma@mail.ru

УДК 519.688

THE SOFTWARE TO TEST COMPONENTS OF THE INTEGRATED SECURITY SYSTEMS OF NPP OF DIFFERENT DEVELOPERS ON THE INTEGRATION

Bezuglov D.Y.*, Trofimov M. A.**

*ATEKS Ltd. 11, Lubogo St., ap. 149, Obninsk, Kaluga reg., 249038 Russia
**Obninsk Institute for Nuclear Power Engineering, National Nuclear Research University «MEPhI». 1 Studgorodok, Obninsk, Kaluga reg., 249040 Russia

ABSTRACT

Physical protection of nuclear power plants provide an Integrated security system. Often the integration is reduced to developed specific solutions for interoperability between products from the same developer. In 2009, the standard was instituted JSC «Concern Rosenergoatom» STO 1.1.1.04.007.0814-2009. The aim of this standard is the solution to the problem of compatibility of the products of different developers. Compliance with this standard is confirms by certification. The automated stand and specialized software «AtomTest» was developing with the execution of works on certification. The program is working on the principle of the proxy server. The mechanism retransmission communication through standardized protocols between software components of the integrated security systems had been developing.

According to the test plan «AtomTest» connects, user notification, the expectation criteria continue, then you change the port number and, if available, the IP address set in the configuration bench computer, interception of messages circulating between software components, and substitute them in meaningful information.

When testing the program is providing: scan network traffic for compliance with UTF-8 encoding, syntax, and semantics of XML, XSD schema build commands and command sequences.

After testing the program is analyzing event log, with subsequent reporting format .html and .pdf then print. The steps are performed automatically without operator intervention.

According to the results of work performed six developers has gained certificates of compliance. This suggests the possibility of integration of components, integrated systems from different developers. It should also be noted the importance of further work in this direction.

Key words: Physical security, Integrated security system, the industry standard, automated facility, network traffic, standardized protocols, machine States, specialized software.

REFERENCES

1.Sevryukov D.V., Asfandiyarov A.H. The safety of nuclear and radiation facilities. *Bezopasnost' okruzhayuschej sredy*. 2007, no. 3, pp. 12-18 (in Russian).

2. Zwierzynski S. The problem of choice of perimeter detection equipment. Part 1. *Bezopasnost'. Dostovernost'. Informaciya*. 2002, no. 4 (44). (in Russian).

3. Garcia M. Design and evaluation of physical protection systems. Moscow. Mir, LLC «Izdatelstvo AST» Publ., 2003. 386 p. (in Russian).

4. Magauenov RG Alarm system: basic theory and principles of construction. Moscow. «Goryachaya Liniya – Telecom» Publ., 2004. 367 p. (in Russian).

5. JSC «Concern Rosenergoatom» Standard SRT 1.1.1.04.007.0814-2009 «Collection system, and addressing complex information-processing engineering systems of physical protection of nuclear power plants». Technical requirements. Enacted by the order of JSC «Concern Rosenergoatom» № 1782 from 17.12.2009 (in Russian).

6. Omel'yanchuk A.M. Standarty na integrirovannye sistemy bezopasnosti – vzglyad razrabotchika. Chast' 2 [Standards for integrated security systems – Developer's view. Part 2]. *Security systems*. 2006, no. 1. pp. 116-120 (in Russian). Available at: http://www.secuteck.ru/articles2/kompleks_sys_sec/standarty_na_integrirovannye_sist/

7. Krahmalyov A.K. Eschyo raz ob integracii system bezopasnosti [Exe times on the integration of security systems] *Sec.Ru*. 26.05.2014 (in Russian). Available at: http://daily.sec.ru/2014/05/26/Eshe-raz-ob-integratsii-sistem-bezopasnosti.html

Authors

Bezuglov Dmitrij Yur'evich, Specialist ATEKS Ltd, PhD Student
E-mail: d1.bezuglov@gmail.com

Trofimov Maksim Adol'fovich, Professor, Dr. Sci. (Engineering)
E-mail: trofimovma@mail.ru