УДК 004.056.5

П.А. Смольянинов, Г.А. Кравцов, Киев

БАЗОВАЯ МОДЕЛЬ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ УПРАВЛЕНИЯ ИНДУСТРИАЛЬНЫХ СИСТЕМ И ИХ БЕЗОПАСНОСТЬ

Abstract. It is described model of basic operations of industrial control systems (ICS) which is presented in the NIST SP 800-82 standard and described developed the base model of the information management process which presents this process in the form of set of various information and operations with this information is developed.

Актуальность проблемы

Актуальность проблемы обеспечения информационной безопасности (ИБ) ключевых систем, входящих в состав критически важной информационной инфраструктуры Украины, обуславливается такими современными условиями ведения деятельности на объектах информационной и телекоммуникационной инфраструктуры государства как [1]:

– наличие растущей зависимости бизнес-процессов от информационно-коммуникационных технологий;

– сложность используемых технологий;

– большое количество потенциальных угроз ИБ, включая терроризм.

Реализация обозначенных угроз может приводить к значительным негативным последствиям для безопасности государства в информационной сфере и препятствовать реализации Украиной своих целей во внутренней/внешней политике.

Основная часть

1. ИНДУСТРИАЛЬНЫЕ СИСТЕМЫ УПРАВЛЕНИЯ И ИХ БЕЗОПАСНОСТЬ

Индустриальные (промышленные) системы автоматизации и управления (Industrial Control Systems, далее ICS) [2] являются основными компонентами инфраструктуры современных предприятий, принадлежащим к различным секторам экономики (топливно-энергетический комплекс, металлургическая промышленость, химическая промышленность и др.) и могут включать в себя системы управления производственными процессами (MES, Manufacturing Execution System), системы диспетчерского управления и сбора данных (SCADA, Supervisory Control And Data Acquisition), системы управления, построенные на базе программируемых логических контроллеров (PLC, Programmable Logic Controller), и др.

Обеспечение информационной безопасности промышленных систем автоматизации и управления как критически важных элементов бизнес-процессов, является неотъемлемой частью процесса обеспечения безопасности

предприятия в целом.

В настоящее время, при развитии и модернизации предприятий, в промышленных системах внедряются унифицированные технологии (IP/Ethernet), новые сервисы (виртуализация, IP-телефония, мобильность и др.), повышается уровень автоматизации технологических процессов и осуществляется интеграция с системами управления предприятием (ERP, Enterprise Resource Planning). В свою очередь, повышение уровня автоматизации может привести и к увеличению вероятности реализации известных угроз, и к появлению новых угроз безопасности.

Важно отметить, что, в течение последних десяти лет, наблюдается значительный рост количества инцидентов и выявленных уязвимостей, а также целенаправленных атак на промышленные системы автоматизации и управления, целью которых являются промышленный шпионаж, мошенничество и нарушение функционирования предприятия.

Обеспечение безопасности промышленных систем автоматизации и управления – сложная задача, требующая комплексного подхода, для решения которой необходимо учитывать и специфику промышленных систем (в том числе, и использование устаревших и уязвимых компонентов, протоколов, требования к надежности и непрерывности функционирования, климатические условия и др.), международные стандарты и лучшие практики (IEC 62443 (ISA 99), CIP NERC, NIST и др.) В рамках комплексного подхода по обеспечению безопасности промышленных систем автоматизации и управления решаются задачи защиты обрабатываемой информации, обеспечения непрерывности функционирования технологических процессов, а также противодействие мошенничеству и хищению.

Схематически произвольная ICS [3,4] может быть представлена схемой (рис. 1).

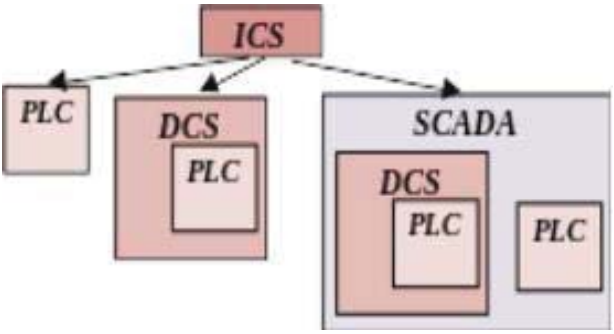

Рис. 1. Разновидности ICS

2. БАЗОВАЯ МОДЕЛЬ ОПЕРАЦИЙ *ICS* (*NIST Special Publication 800-82, Guide to ICS Security*)

Очевидно, ***ICS*** **–** это большое разнообразие топологий. ***Базовая модель операций ICS*** – отображает сущность процессов управления в топологиях

ICS и их основное отличие от систем информационных технологий (*ITsystems, ITS*)

В рамках современных подходов кибернетики при представлении процессов управления в технических, биологических и социальных системах применяются известные модели, основанные на информационном взаимодействии субъекта и объекта управления. Типичным примером такого представления является модель базовых операций индустриальных систем управления (basic operation of an ICS) [5,6], которая представлена на рис. 2.

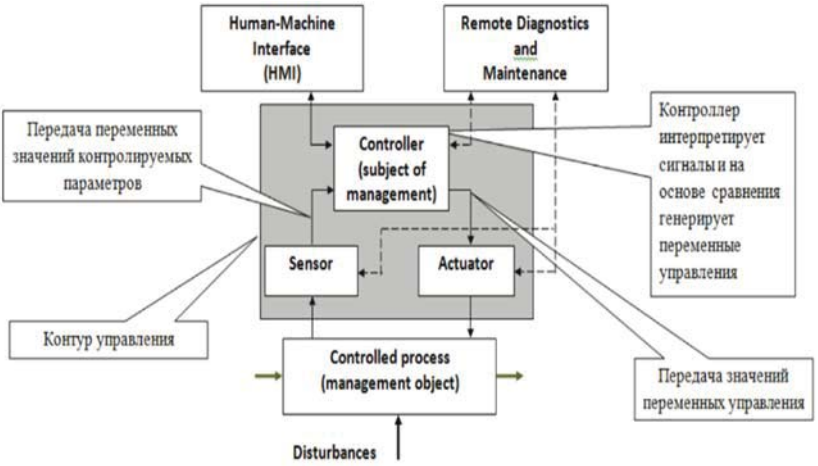

Рис. 2. Модель базовых операций индустриальных систем управления

Таблица 1

Разновидности ICS

PLC	*Programmable Logic Controller*	программируемый логический контроллер (управление выделенными объектами)
DCS	*Distributed Control Systems*	распределённая система управления (совместное управление локально распределёнными объектами)
SCADA	*Supervisory Control and Data Acquisition system*	диспетчерская система управления и сбора данных (совместное управление удалённо распределёнными объектами)

При анализе вопросов безопасности с помощью комбинаций данной модели можно представить контуры управления (control loops)

индустриальных систем различных видов и сложности, например: программируемых логических контроллеров (PLC), распределенных систем управления (DCS), диспетчерских систем управления и сбора данных (SCADA). Однако, такая модель не позволяет в явном виде представить информационный процесс управления. В рамках существующей парадигмы информационной безопасности, когда безопасности связывается с обеспечением свойств информации (конфиденциальность, целостность, доступность и др.), при определении и анализе уязвимостей важно знать о какой информации и каких этапах управления ведётся речь.

3. БАЗОВАЯ МОДЕЛЬ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ КИБЕРНЕТИЧЕСКОЙ СИСТЕМЫ

Наиболее иллюстративным является отчет Лаборатории Касперского [7]. Согласно указанному отчету, наиболее известными уязвимостями и их реализациями являются:

- NTP Symmetric Association Authentication Bypass Vulnerability (CVE-2015- 7871);
- Glibc Ghost Vulnerability (CVE-2015-0235);
- Multiple Mango Automation 2.6.0 Vulnerabilities;
- Authentication Bypass Vulnerability (CVE-2015-7938);
- Multiple Janitza UMG Power Quality Measuring Products Vulnerabilities;
- AMX Multiple Products Credential Management Vulnerability;
-Yokogawa CENTUM CS 3000 Buffer Overflow Vulnerability;
- Elipse E3 DLL Hijacking Vulnerability;
- SearchBlox v8.3 Information Exposure Vulnerability;
- Moxa VPort ActiveX SDK Plus Buffer Overflow Vulnerability.

Следует осознать, что 85% уязвимостей создают ошибки при разработке программного обеспечения.

Понимание природы возможных уязвимостей дают следующие данные [2]:

Таблица 2

Уязвимости в ICS

ICS Component Types	High risk level, %	Medium risk level, %	Low risk level, %
HMI	23%	13%	7%
Electric Device	16%	7%	
SCADA	16%	25%	2%
Network Device	13%	11%	1%
Controller	10%	4%	3%
Web Server	7%	1%	

OPC Server	5%	1%	
Base Station	4%		
DCS	3%		
RTU	2%	1%	
Communication Module	1%	2%	
Search Engine	1%		
Vehicle-based infotainment systems	1%		
OS		8%	2%
Mobile Application		3%	3%
Thermal Calculation Software		2%	
System Platform		1%	

При этом ТОП-8 уязвимостей представлены следующим списком:

- Buffer Overflow (Переполнение буфера) – ошибка программирования, где программное обеспечение, при записи данных в буфер, превышает границу буфера и перезаписывает смежные ячейки памяти. Запись снаружи границы блока выделенной памяти может повредить данные, нарушить работоспособность программы или позволит выполнение вредоносного кода.

- Hard-Coded Credentials (Жестко-закодированные учетные данные) – такие как пароль или криптографический ключ, создают значительную брешь в системе безопасности, которая позволяет злоумышленнику обходить настроенную администратором (разработчиком) программного обеспечения аутентификацию.

- The Cross-Site Request Forgery (Межсайтовая подделка запроса) – уязвимость существует, когда веб-сервер сконфигурирован таким образом, чтобы получать запрос от клиента без какого-любого механизма для проверки, при этом запрос со стороны пользователя отправляется принудительно и без его ведома.

- Improper Input Validation (Неправильная проверка ввода или непроверенный пользовательский ввод) – программные продукты (программное обеспечение) содержащую эту уязвимость, не проверяют, или некорректно проверяют входные данные, которые могут влиять на поток управления или поток данных программы. Большая часть эти дефектов (уязвимостей) связаны с дальнейшим произвольным выполнением кода.

- Cleartext Transmission of Sensitive Information (Передача в открытом виде чувствительной информации) – уязвимость позволяет несанкционированному пользователю прослушивать и перехватывать

чувствительную информацию (критические данные) в канале связи, поскольку программное обеспечение передает такие данные в открытом виде.

- Storage of Passwords in a Recoverable Format (Хранение паролей в формате, позволяющем произвести их восстановление) – хранение паролей в открытом виде или со помощью алгоритмов со слабой стойкостью.

- Unrestricted File Upload (Отсутствие ограничений на загрузку файла) – позволяет атакующему загружать или передавать файлы разных типов, которые могут быть автоматически обработаны программным продуктом (программным обеспечением).

- SQL Injection (SQL инъекция или внедрение SQL-кода)– уязвимость, которая позволяет производиться вставку дополнительных данных (подготовленных заранее злоумышленником) в SQL запрос на сервер, с целью обработки этих данных на стороне сервера.

- и другие.

Чтобы понять суть указанных уязвимостей, следует обратиться к базовой модели информационного процесса управления (см. рис.3) [5,8], которая представляет этот процесс в виде совокупности различных информаций и операций с этой информацией.

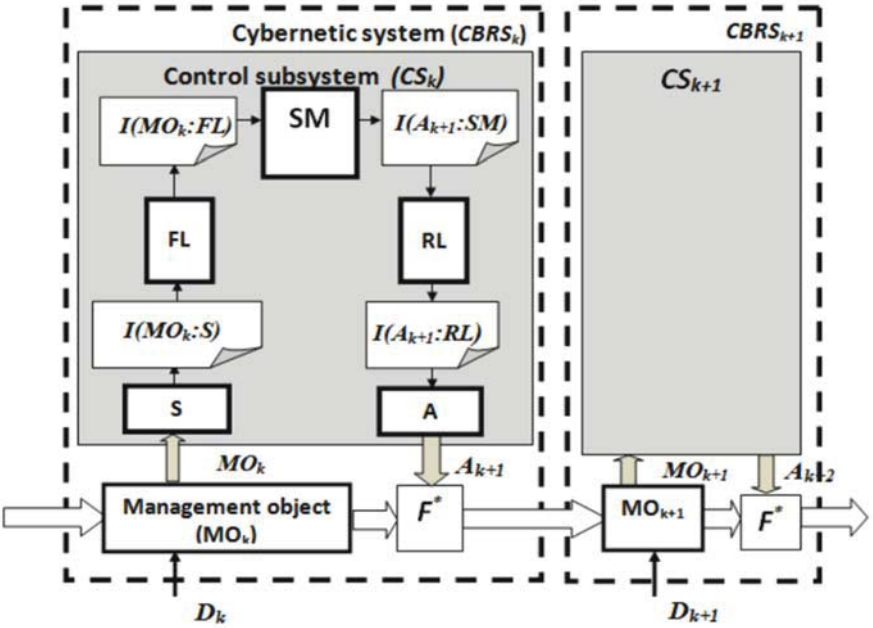

Рис. 3. Базовая модель информационных процессов управления

Модель отображает следующие процессы:

1. текущая k-я фаза состояния кибернетической системы CBRSk определяется состоянием объекта управления MOk, на который оказывается

воздействие внешней среды;

2. сенсор S отображает это состояние в формируемой информации I(MOk:S), которая передаётся по прямому каналу связи FL (Forward Link);

3. с выхода канала связи на вход субъекта управления SM (Subject of Managment) поступает принятая информация о состоянии объекта управления I(MOk:FL);

4. по результатам оценки состояния объекта управления SM принимает решение о следующем (k+1)-ом состоянии объекта управления, которое отображается в формируемой информации I(Ak+1:SM);

5. принятое решение через обратный канал связи RL (Reverse Link) подается на исполнительное устройство A (actuator, актуатор), которое преобразует эту команду в исполнительное воздействие на объект управления;

6. объект управления под заданным воздействием переходит в следующее состояние (MOk+1 = F*(MOk, Ak+1), где F*(.) – оператор перехода). Момент времени окончания перехода является границей между k-й и (k+1)-ой фазами.

Принято сравнивать указанную модель с моделью базовых операций индустриальных систем управления :

1. вместо совокупности понятий «контур управления» и «субъект управления» предлагаются группа «вложенных в друг друга» понятий: «управляемая (кибернетическая) система», «подсистема управления» и «субъект управления»;

2. процесс управления, представленный в виде последовательности устройств (сенсор, контроллер (субъект управления), актуатор), связанных между собой передаваемыми сигналами с текущими значениями параметров объекта управления, заменяется информационным процессом управления. Этот процесс представлен в виде последовательности операций над исходной информацией об объекте управления. Исходная, промежуточные и конечная информация процесса содержат в принятых обозначениях сведения о референте информации и об этапе управления, на котором эта информация рассматривается.

Выводы

Предложенная модель может быть применена для формализованного анализа безопасности информационных процессов в индустриальных системах управления с контурами управления различной сложности. Модель позволяет конкретизировать уязвимости по месту расположения информации в системе и свойствам этой информации, наличие которых отвечает критериям безопасности.

1. *Леоненко Г. П., Юдин А. Ю.* Проблемы обеспечения информационной безопасности систем критически важной информационной инфраструктуры Украины // Information

Technology and Security. – 2013. – Вип. 1(3). – С.44.
2. Безопасность промышленных систем автоматизации и управления [Электронный ресурс]. – Режим доступу: http://www.ussc.ru/catalog/id/26
3. Data Historians vs. DCS, SCADA, and PLC Systems [Электронный ресурс] – Режим доступу : http://instrumentationandcontrol.net/wp-content/uploads/2016/05/ASPENTECH-2013-Data-Historians-vs.-DCS-SCADA-and-PLC-Systems.pdf
4. The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress [Электронный ресурс] – Режим доступа:https://fas.org/sgp/crs/misc/R42984.pdf
5. *Яковив И. Б.* Базовая модель информационных процессов управления и критерии безопасности кибернетической системы/ И.Б. Яковив// Інформаційні технології і безпека : збірник наукових праць. – К. : ІССЗІ НТУУ «КПІ», 2015. – Випуск No 2 (4). – С.68-74.
6. National Institute of Standards and Technology (2013), NIST Special Publication 800-82. Revision 1, Guide to Industrial Control Systems (ICS) Security, available at : http://dx.doi.org/10.6028/NIST.SP.800-82r2 (May 2015).
7. Отчет Лаборатории Касперского INDUSTRIAL CONTROL SYSTEMS VULNERABILITIES STATISTICS [Электронный ресурс). – Режим доступу : https://kasperskycontenthub.com/securelist/files/2016/07/KL_REPORT_ICS_Statistic_vulnerabilities.pdf
8. *Яковив И. Б.* Канал связи с позиций атрибутивно-трансфертной сущности информации / И. Б. Яковив // Інформаційні технології і безпека : збірник наукових праць. – К.: ІССЗІ НТУУ «КПІ», 2012. – Випуск No 2 (2). – С.84-96.

Поступила 11.09.2017р.

УДК519.711

Ю.Г. Куцан, Г.А. Иванов, Киев

МОДЕЛИРОВАНИЕ РАЗВИТИЯ РЫНОЧНЫХ МЕХАНИЗМОВ ЦЕНООБРАЗОВАНИЯ В УСЛОВИЯХ НОВОГО ЛИБЕРАЛИЗИРОВАНОГО РЫНКА ЭЛЕКТРИЧЕСКОЙ ЭНЕРГИИ УКРАИНЫ

Abstract. The presented research is aimed at studying approaches and methods for regulating the liberalized electricity market in order to model the contractual relations of its participants and to model pricing for electricity and related transportation and supply services. In addition, the study will help to better understand the relationship with the pricing of the respective energy market segments, and also to determine the long-term prospects of the Ukrainian electricity market.

Ключевые слова: рынок электрической энергии, либерализация, конкуренция, модель рынка электроэнергии, потребитель электрической энергии, переход к новой модели рынка, европейская модель рынка.

