CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION

УДК 621.391

ИГОРЬ ЯКОВИВ

БАЗОВАЯ МОДЕЛЬ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ УПРАВЛЕНИЯ И КРИТЕРИИ БЕЗОПАСНОСТИ КИБЕРНЕТИЧЕСКОЙ СИСТЕМЫ

Актуальной является задача разработки универсальных средств формализованного анализа уязвимостей информационных процессов систем различной физической природы. Предложена базовая модель информационных процессов кибернетической системы. Получены математические выражения, описывающие сущность безопасности кибернетической системы и формализованные критерии этой безопасности.

Ключевые слова: безопасность кибернетической системы, информационный процесс, анализ уязвимостей, критерии безопасности.

Угрозы безопасности информационных процессов и кибернетические системы. Среди актуальных угроз национальной безопасности [1] непосредственное отношение к сфере обеспечения безопасности информационных процессов имеют следующие:

- угрозы ведения информационно-психологической войны против Украины;
- угрозы кибербезопасности и безопасности информационных ресурсов;
- угрозы безопасности управления объектами критической инфраструктуры.

Целью информационно-психологического воздействия через электронные средства массовой информации является манипуляция сознанием граждан, обострение внутриполитической ситуации в стране. Применение кибератак может привести к нарушениям работы информационно-телекоммуникационных систем, изменениям, блокированию или уничтожению информационных ресурсов, непосредственному нанесению материального и морального вреда пользователям услуг компьютерных систем. Злоумышленные вмешательства в работу систем управления объектами критической инфраструктуры могут привести к прямому негативному воздействию на физический мир. Результаты такого воздействия связаны со значительными рисками для здоровья и жизни людей, серьёзным ущербом окружающей среде, негативным влиянием на финансы и экономику страны.

Несмотря на значительные различия в природе тех нежелательных событий, которые становятся результатами атак, интуитивно понятно, что общей основой этих угроз является негативное вмешательство в информационные процессы. Представляется актуальной задача формирования единой системы взглядов на безопасность информационных процессов, используемых в различных сферах. Такой подход может позволить сформировать на основе общих теоретических позиций методы конструктивного анализа недостатков (уязвимостей) информационных систем различной физической природы и разрабатывать аргументировано обоснованные меры результативного противодействия информационным атакам.

Информационный процесс, сущность информации и кибернетическая система. В статье предлагается один из возможных подходов формирования системы взглядов на безопасность информационных процессов. В основе его лежат следующие предлагаемые утверждения:

– информационный процесс следует рассматривать в рамках управляемой (кибернетической) системы (далее – c*ontrolled system* или *cybernetic system, CBRS*);

– кибернетическая система состоит из управляемого объекта (*management object, MO)* и подсистемы управления *(control subsystem, CS);*

– основой подсистемы управления является субъект управления (*subject of management, SM*), который на основании информации о текущем состоянии объекта управления принимает решение о последующем состоянии этого объекта;

– информация об объекте А в объекте В (далее – *I(A:B)*) – это свойства объекта А, отображённые в другом объекте В. Относительно информации *I(A:B)* объект А – это референт информации (*referent I(A:B)*), т.е. тот объект, образ которого отображен в информации, а объект В – это носитель информации об объекте А (*carrier I(A:B)*);

– управляющий информационный процесс – это последовательность следующих операций с информацией в подсистеме управления:

1) формирование информации о текущем состоянии объекта управления *MO*;

2) передача сформированной информации субъекту управления *SM*;

3) оценка субъектом управления *SM* принятой информации и принятие решения о последующем состоянии объекта управления;

4) передача объекту управления информации о решении субъекта управления;

5) реализация объектом управления принятого решения.

Таким образом, предложенная система взглядов на информационные процессы в любых сферах деятельности представляет их как управляющие процессы в рамках кибернетической системы, причём информация в них рассматривается как результат отображения свойств одних объектов в других (применён атрибутивно-трансфертный подход к сущности информации [2]).

Модели процесса управления. 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*) [3], которая представлена на рис. 1.

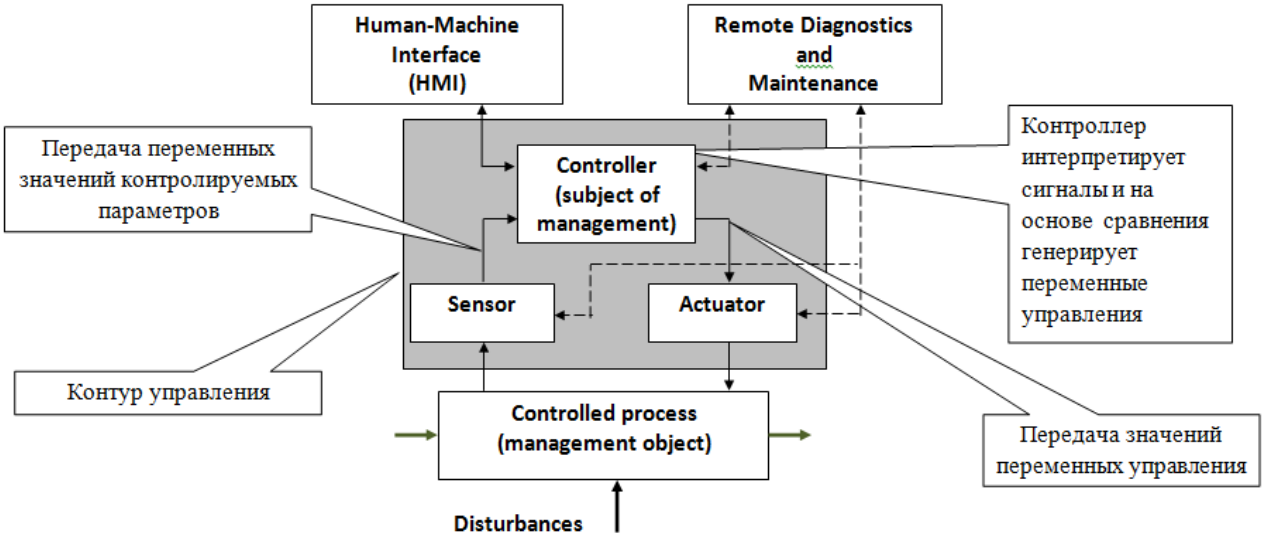

Рисунок 1 – Модель базовых операций индустриальных систем управления

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*), распределённых 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.

Базовая модель информационных процессов кибернетической системы. С предложенных выше позиций (пункт 2) в рамках дальнейшей формализации была получена *базовая модель информационного процесса управления* (см. рис.2), которая представляет этот процесс в виде совокупности различных информаций и операций с этой информацией. Причем, такая модель позволяет также обозначить и смысл (семантику) информации, применяемой на различных этапах процесса управления.

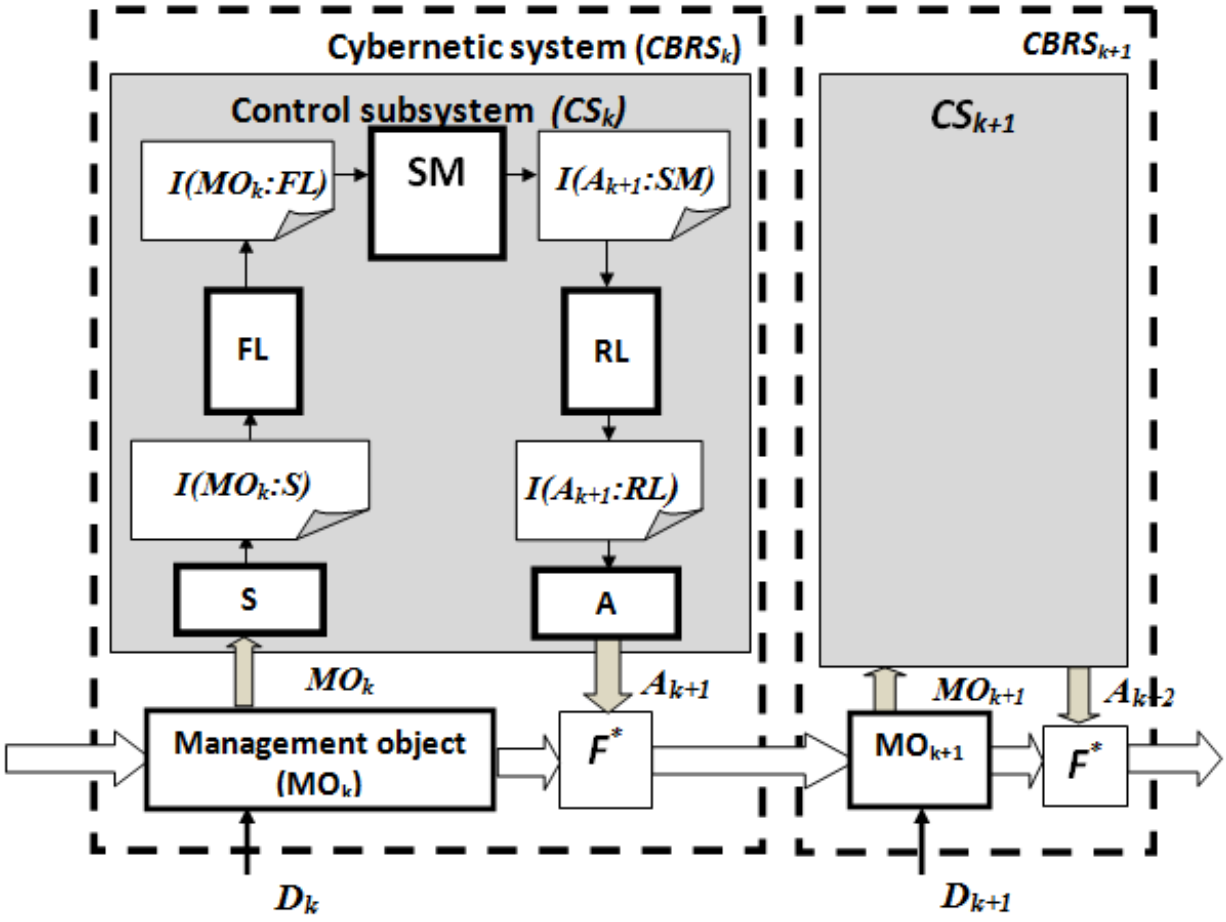

Рисунок 2 – Базовая модель информационных процессов управления

Модель отображает следующие процессы:

– текущая *k*-я фаза состояния кибернетической системы $CBRS_k$ определяется состоянием объекта управления MO_k, на который оказывается воздействие внешней среды D_k;

– сенсор S отображает это состояние в формируемой информации $I(MO_k:S)$, которая передаётся по прямому каналу связи FL (*Forward Link*);

– с выхода канала связи на вход субъекта управления SM поступает принятая информация о состоянии объекта управления $I(MO_k:FL)$;

– по результатам оценки состояния объекта управления SM принимает решение о следующем $(k+1)$-ом состоянии объекта управления, которое отображается в формируемой информации $I(A_{k+1}:SM)$;

– 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;

– объект управления под заданным воздействием переходит в следующее состояние ($MO_{k+1} = F^*(MO_k, A_{k+1})$, *где* $F^*(.)$ *– оператор перехода*). Момент времени окончания перехода является границей между *k-й* и $(k+1)$*-ой* фазами.

Основные отличия предложенной модели от известной модели базовых операций индустриальных систем управления следующие:

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

– *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.

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

Критерии безопасности кибернетической системы. В качестве примера результативного применения предложенной модели был получен формализованный критерий безопасности кибернетической системы. С этой целью в общем виде было предложено математическое описание кибернетической системы:

$$\begin{cases} MO_{k+1} = F^{*}(MO_k, A_{k+1}); \\ A_{k+1} = F_{cs}(MO_k). \end{cases} \quad (1)$$

где $F^{*}(.)$ – оператор перехода объекта управления, $F_{cs}(.)$ – оператор управления. Такое представление можно назвать *моделью поведения кибернетической системы.*

Пусть в рамках этой модели MO_k и A_{k+1} принимают соответственно значения $x_m^{(MO)} \in \{x_m^{(MO)}\} = \Omega_{MO}$ и $x_i^{(A)} \in \{x_i^{(A)}\} = \Omega_A$, где множества Ω_{MO} и Ω_A – алфавиты контролируемых состояний и допустимых исполняющих воздействий. Индексы m и i – номера элементов этих алфавитов. Тогда правило (закон) управления $F_{cs}(.)$, реализуемое подсистемой управления *CS*, можно описать бинарным отношением

$$F_{cs} = \{(x_m^{(MO)}, x_i^{(A)})\} \subset \Omega_{MO} X \Omega_A. \quad (2)$$

В соответствии с выражением (2) можно утверждать, что управляющее воздействие A_{k+1} принимает только то значение $x_i^{(A)}$, которое задаётся правилом управления F_{cs} при поступившем значении $x_m^{(MO)}$ состояния объекта управления MO_k. Все другие значения A_{k+1}, которые не соответствуют этому правилу управления при значении $x_i^{(A)}$, являются несанкционированными и приводят к нарушению поведения кибернетической системы. Такая система не является безопасной.

Предложенные выше представления позволяют математически записать «функцию безопасности кибернетической системы», которую обозначим как *SEC(.)*:

$$SEC(MO_k, A_{k+1}) = \exists\, MO_k\, ((MO_k, A_{k+1}) \in F_{cs}). \quad (3)$$

Данная функция может принимать только два значения: 1 – если значение управляющего воздействия соответствует принятому правилу управления; 0 – если не соответствует, т.е.

$$SEC(MO_k, A_{k+1}) \in \{0, 1\}. \quad (4)$$

Предложенная математическая формализация позволяет сформулировать следующее определение:

безопасность кибернетической системы *– это такое её состояние, при котором преднамеренное несанкционированное воздействие на неё не приводит к нарушению поведения объекта управления.*

В этом случае критерием безопасности кибернетической системы будет значение (1 или 0), которое принимает функция $SEC(MO_k, A_{k+1})$.

Примечание: влияние неблагоприятных естественных воздействий на техническую кибернетическую систему учитывается ещё на этапе разработки правил управления, что и определяет устойчивость таких систем к изменениям окружающей среды. Целесообразно учёт этих факторов относить к проблемам надёжности системы. При рассмотрении вопросов безопасности следует ограничиться только преднамеренными несанкционированными воздействиями. Уточнение вопросов безопасности кибернетических систем биологической и социальной природы требует дополнительных исследований в сфере формализации психических реакций (принятие решений на основе безусловных и условных рефлексов, интеллектуальных актов разного уровня).

Критерии безопасности информационных процессов индустриальных систем управления. Индустриальные системы управления (*IndustrialControlSystem, ICS*) составляют значительную часть объектов критической инфраструктуры и относятся к классу технических кибернетических систем. Информационные процессы таких систем в подавляющем большинстве реализуются на основе совокупности электронных устройств различной сложности. Актуальным представляется получить определение безопасности такого процесса и её формализованные критерии.

В рамках предложенной *базовой модели информационных процессов кибернетической системы* (рис.2) границами такого процесса можно считать информации $I(MO_k:S)$ и $I(A_{k+1}:RL)$. В общем виде математическое представление такого процесса может быть следующим:

$$\begin{cases} I(MO_k:FL) = F_{FL}\,[I(MO_k:S)], \\ I(A_{k+1}:CS) = F_{CS}\,[I(MO_k:FL)], \\ I(A_{k+1}:RL) = F_{RL}[I(A_{k+1}:CS)], \end{cases} \quad (5)$$

где:

$F_{FL}[.]$ – оператор передачи информации о состоянии объекта управления;

$F_{CS}[.]$ – оператор принятия решения;

$F_{RL}[.]$ – оператор передачи команды управления.

Если принять во внимание то, что сенсоры в таких системах обеспечивают взаимно однозначное соответствие между MO_k и $I(MO_k:S)$, а актуаторы – такое же соответствие между $I(A_{k+1}:RL)$ и A_{k+1}, то по аналогии с (3) можно записать «*функцию безопасности информационного процесса ICS*»

$$SEC_{ICS}\,[I(MO_k:S), I(A_{k+1}:RL)\,] = \exists\, I(MO_k:S)\{[I(MO_k:S), I(A_{k+1}:RL)\,] \in F^*_{cs}\} \quad (6)$$

где F^*_{cs} правило управления (принятия решения), задающее соответствие между значениями $I(MO_k:S)$ и $I(A_{k+1}:RL)$.

Теперь введём следующие взаимосвязанные определения:

информационная среда ICS *(information medium ICS)* – совокупность электронных средств ICS, реализующих информационные процессы управления;

безопасность информационного процесса ICS – это такое состояние управляющей подсистемы (*CS*), при котором преднамеренное несанкционированное воздействие на информационную среду *ICS* не приводит к незапланированному поведению объекта управления.

По аналогии с (4) формализованным критерием безопасности информационного процесса *ICS* будут значения, которые принимает функция

$$SEC_{ICS}\,[I(MO_k:S), I(A_{k+1}:RL)\,] \in \{0, 1\}. \quad (7)$$

Заключение. На основе предложенных представлений о сущности информации и информационных процессов разработана модель информационных процессов кибернетической системы. На основе этой модели получены:

математические выражения, описывающие сущность безопасности кибернетических систем и информационных процессов индустриальных систем управления:

формализованные критерии безопасности.

Полученные результаты могут применяться в качестве универсального инструментария для формализованного анализа уязвимостей информационных процессов организационно-технических и технических систем. Такой анализ позволяет конкретизировать уязвимости по месту расположения информации в системе и свойствам информации, наличие которых соответствует критериям безопасности.

Перспективными представляются исследования в следующих направлениях:

– разработка методик информационно-функционального анализа индустриальных систем управления различной сложности;

– разработка базовой модели неблагоприятного информационно-психологического воздействия с помощью Internet, методик результативного противодействия;

– разработка базовой модели уязвимостей компьютерной информационной среды;

– разработка методов и средств противодействия неблагоприятному информационно-психологическому воздействию в сферах применения цифровых фото- и видеоизображений.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Стратегія національної безпеки України [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/105/2007. – Дата доступу : березень 2015. – Назва з екрану.

2. 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 № 2 (2). – С. 84-96.

3. Guide to Industrial Control Systems (ICS) Security : NIST Special Publication 800-82. Revision 1 [Electronic resource]. – Access mode : http://dx.doi.org/10.6028/NIST.SP.800-82r1. – Access data : January 2015. – The title of the screen.

Статья поступила в редакцию 23.03.2015.

REFERENCE

1. National Security Strategy of Ukraine (2007), available at : http://zakon4.rada.gov.ua/laws/show/105/2007 (accessed 20 March 2015).

2. Yakoviv, I. B. (2012), *The communication channel from the positions of attributive-transfer nature of the information* [*Kanal sviazi s pozitcii atributivno-transfertnoi sushchnosti informatcii*], Information technology and security, No. 2 (2), pp. 84-96.

3. 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.800-82r1 (accessed 13 January 2015).

ІГОР ЯКОВІВ

БАЗОВА МОДЕЛЬ ИНФОРМАЦІЙНИХ ПРОЦЕСІВ УПРАВЛІННЯ ТА КРИТЕРІЇ БЕЗПЕКИ КІБЕРНЕТИЧНОЇ СИСТЕМИ

Актуальним завдання розробки універсальних засобів аналізу вразливостій інформаційних процесів систем різної фізичної природи. Запропоновано базова модель інформаційних процесів кібернетичної системи. Отримано математичні вирази, що описують сутність безпеки кібернетичної системи і формалізовані критерії цієї безпеки.

Ключові слова: безпека кібернетичної системи, інформаційний процес, аналіз вразливостей, критерії безпеки.

IGOR YAKOVIV

THE BASE MODEL OF INFORMATIONAL PROCESSES OF MANAGEMENT AND SAFETY CRITERIA FOR CYBERNETIC SYSTEMS

Actual is the task of the development of universal tools formalized analysis of complex vulnerabilities of information systems processes of different physical nature. The article proposed a model of the information processes of a cybernetic system. The article also presents mathematical expressions that describe the essence of security of cyber systems and formal criteria for this security.

Keywords: security of cyber systems, information process, vulnerability analysis, security criteria.

Игорь Богданович Яковив, кандидат технических наук, доцент кафедры кибербезопасности и автоматизированных систем и технологий, Институт специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт», Киев, Украина.

E-mail: iyakov52@gmail.com.

Ігор Богданович Яковів, кандидат технічних наук, доцент кафедри кібербезпеки та автоматизованих систем і технологій, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут», Київ, Україна.

Igor Yakoviv, candidate of technical sciences, assistant professor, department of cyber security and automated systems and technology, Institute of Special Communication and Information Protection of National Technical University of Ukraine «Kyiv Polytechnic Institute», Kyiv, Ukraine.