МОДЕЛЬ ФУНКЦИОНИРОВАНИЯ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ В КИБЕРПРОСТРАНСТВЕ

Захарченко Р.И.¹, Королев И.Д.²

Целью работы является формализация процесса функционирования автоматизированной информационной системы специального назначения (далее по тексту АИС) в киберпространстве. В условиях информационного противоборства АИС рассматривается как сложная многоуровневая иерархическая система, а процесс ее функционирования декомпозируется до отдельных сетевых сервисов и обеспечивающих их функционирование протоколов по уровням модели OSI.

Используемые методы. При разработке модели были использованы методы теории динамических систем, теории конфликта и теории сложных иерархических систем.

Новизна. Элементом новизны разработанной модели является представление АИС в виде сложной иерархической модели с описанием динамических процессов, учитывающей одноуровневые и разноуровневые функциональные отношения между элементами АИС (сетевыми сервисами, техническими средствами обработки информации) и системами управления АИС и информационно-техническими воздействиями в соответствии с моделью OSI. Данные отношения рассматриваются в условиях информационного противоборства в киберпространстве с учетом показателей качества функционирования сетевых сервисов и ресурсов, необходимых для обеспечения функционирования и осуществления на сетевые сервисы как конструктивных, так и деструктивных воздействий.

Результаты и их значимость. Разработанная модель АИС в киберпространстве может быть использована для разработки новых стратегий управления АИС с учетом противодействия информационно-техническим воздействиям в киберпространстве.

Ключевые слова: модель АИС, информационно-техническое воздействие, информационный конфликт, модель OSI.

DOI: 10.21681/2311-3456-2019-6-69-78

Введение

Функционирование автоматизированной информационной системы специального назначения (АИС) в киберпространстве в условиях информационно-технического воздействия (ИТВ) порождает новые уязвимости и угрозы [1] и требует разработки нового инструментария обеспечения ее устойчивого функционирования [2]. Необходимо отметить, что для разработки данного инструментария необходимо исследовать процессы антагонистического взаимодействия иерархических организационно-технических систем, стремящихся распространить управляющие воздействия друг на друга через совместно используемый общий ресурс (киберпространство), а затем решить проблему синтеза соответствующей модели [3].

Такая особенность АИС, как обработка сведений ограниченного распространения, определяет способ ее интеграции, при котором элементы АИС находятся в пределах контролируемой зоны, а каналы передачи

данных между ними в киберпространстве физически или логически выделены и защищены криптографически, что значительно ограничивает возможности злоумышленников по вмешательству в процессы обработки информации и послужит ограничением при дальнейшем рассмотрении процесса функционирования АИС в киберпространстве [3, 4].

В качестве эффективного средства предметной организации информации о процессе функционирования АИС в киберпространстве целесообразно осуществить его «модельное» представление как организованных знаний, несущих функционально необходимую и достаточно обоснованную системную информацию.

Рассмотрение процесса функционирования АИС в условиях информационного противоборства произведем на основе теории динамических систем в терминологии работ [5, 6] и представим его в виде следующей модели (рис. 1).

1 Захарченко Роман Иванович, кандидат технических наук, докторант, Краснодарское высшее военное училище, г. Краснодар, Россия. E-mail: romanzakharchenko@yandex.ru

2 Королев Игорь Дмитриевич, доктор технических наук, профессор, профессор кафедры, Краснодарское высшее военное училище, г. Краснодар, Россия. E-mail: pi_korolev@mail.ru

Рис. 1. Модель информационного противоборства в киберпространстве

Разработанная модель фиксирует множество возможных априорных и апостериорных знаний о стратегиях противоборствующих сторон и выступает в качестве вербальной (слабо формализованной) модели [7], что позволяет приступить к формализации процесса функционирования АИС в киберпространстве.

В основе формализации данного процесса должен лежать системный подход, позволяющий рассматривать интересующий нас объект – АИС, состоящую из информационных систем (ИС), интегрированных посредством киберпространства, не только как отдельную систему, но и во взаимосвязи с другими системами.

Формализованное представление модели информационного пространства EIS_0 для функционирования АИС в киберпространстве можно выразить следующим образом:

$$EIS_0 = \langle S_0, I, L, C_0, E, P \rangle, \quad (1)$$

где: EIS_0 – киберпространство, $S_0 = \{S_1, \dots, S_n\}$ – конфигурация АИС, представленная в виде совокупности взаимосвязанных ИС, I – модель киберпространства, зафиксированная в форме информационного ресурса, L – характер информационного взаимодействия отдельных ИС в АИС, АИС с средой и взаимодействующими ИС, C_0 – единая цель информационного взаимодействия АИС в киберпространстве (E), E – модель киберпространства для АИС, как совокупности взаимосвязанных ИС $\{S_1, \dots, S_n\}$, P – стратегия (план действий) для изменения или поддержания состояния АИС (S_0).

При этом важно отметить, что необходим анализ не только связей отдельных ИС в целом (АИС) и появляю-

щихся при этом эмерджентных свойств, но и выявление причин их возникновения, т. е. анализ синергетических свойств [8]. Вышесказанное определяет необходимость акцентировать внимание на дальнейшей формализации непосредственно модели функционирования АИС.

Архитектура АИС имеет внутреннюю структуру – взаиморасположение элементов (отдельных ИС) и связей, – задающую устойчивость и воспроизведение выполнения целевой функции. Отдельные ИС, в свою очередь, состоят из элементов (ТСОИ, различающихся свойствами, проявляющимися при взаимодействии), объединенных разнородными связями и вступающими в определенные отношения между собой и средой функционирования, чтобы осуществить процесс (последовательность действий для изменения или поддержания состояния) и выполнить свою целевую (целевые) функцию.

Высокая сложность синтеза адекватной модели функционирования АИС обусловлена следующими особенностями объекта:

- многоуровневой иерархией систем и элементов внутри подсистем с большим количеством разнородных взаимосвязей;
- многочисленностью подсистем и их элементов, объединенных для выполнения заданной целевой функции (функций);
- динамикой изменения целевой функции (функций);
- множественностью математического описания;
- различными видами неопределенностей;
- наличием синергетического эффекта, приводящего к многовариантности состояний подсистем и их элементов (рис. 2).

Рис. 2. Модель представления многовариантного состояния АИС в условия ИТВ

Описание многовариантности состояний АИС представим с точки зрения выходных данных, присущих объекту управления, тогда обобщенное формальное представление модели многовариантного состояния АИС в киберпространстве можно представить в следующем виде:

$$Y = \langle S, C, V, T, R, Z, G, Q \rangle, \quad (2)$$

где: Y – множество выходных данных АИС, S – множество конфигураций АИС определяющих ее текущую структуру и множество функциональных связей, C – множество целей функционирования АИС, V – множество параметров состояния АИС, T – множество моментов времени наблюдения элементов АИС, R – множество ресурсов АИС, $Z = \langle F, X, U \rangle$ – множество воздействий на АИС, F – множество ИТВ на АИС, X – множество воздействий внешней среды на АИС, U – множество управляющих воздействий на АИС, Q – множество показателей качества функционирования АИС, G – критерии способности АИС выполнять целевую функцию.

Таким образом, разработанная модель многовариантного состояния позволяет любое состояние при функционировании АИС описать с достаточной для практики точностью, представив его конечным множеством параметров – индикатором состояния [9], т. е. совокупностью показателей данных значений отдельных ИС и АИС в целом, а затем с использованием методики оценки определить степень достижения текущей цели по соответствующим критериям [10].

Выполним дальнейшую детализацию модели АИС, как сложной иерархической организационно-технической системы, функционирующей в «агрессивной среде». В качестве более ранних работ, которые частично

послужили прототипами общего подхода к моделированию относятся работы Гуревича И.М. [11-13], Вакуленко А.А., Шевчука В.И. [14], Маевского Ю.И. [15]. При этом отдельные уровни разрабатываемой модели соответствуют модели CSI, предложенной Паршуткиным А.В. [16-17], а за ее концептуальную основу взяты представленные в работах Макаренко С.И. двухуровневая модель [18] и динамическая модель связи [19].

Для формализации данной модели введем следующие обозначения:

1) Элементы системы:

$B_{мног}$ – иерархическое представление архитектуры АИС;

m_i – единичный ствол АИС;

n_i – единичный кластер АИС;

o_i – единичный объект АИС (ИС);

a_i – отдельное ТСОИ АИС;

d_i – единичный сетевой сервис или служба, функционирующая в АИС;

c_i – связь между объектами ТСОИ;

$k_{i,j}$ – канал связи между отдельными ИС в АИС;

Предполагается, что канал $k_{i,j}$ соединяет объекты o_i и o_j в случае, если имеются необходимые связи $c_{i1}...c_{in}$, а объектами АИС используются совместные (совместимые) сетевые сервисы, реализованные на протоколах стека TCP/IP;

$l = \overline{1, 7}$ – номер уровня функционирования АИС в соответствии с моделью OSI;

π_i – протокол стека TCP/IP, используемый при функционировании сетевых сервисов и служб АИС;

$\Pi_{d,l} = \{\pi_{d,l,i}\}$ – множество протоколов стека TCP/IP, используемых при функционировании сетевого сервиса d на уровне l модели OSI;

$D(\cdot)$ – область определения ($\cdot$);

e_i – единичный элемент математического обеспечения (алгоритм), используемый в АИС;

$E_{d,l,\pi} = \{e_i | e_i \in D(\pi_{d,l,i})\}$ – множество элементов математического обеспечения (алгоритмов) протокола π_i сервиса d на уровне l модели OSI;

ω_i – параметр элемента математического обеспечения (алгоритма);

$\Omega_{d,l,\pi,a} = \{\omega_i | \omega_i \in D(a), a \in D(\pi_{d,l,i})\}$ –

множество параметров a -ого математического обеспечения (алгоритма) протокола π_i на уровне l модели OSI, реализующих функционирование сервиса d ;

r_i – отдельный вид ресурса АИС;

u_i – управляющее воздействие на АИС со стороны АСУ; f_i – информационно-техническое воздействие со

стороны системы ИТВ;

$R_{d,l,\pi} = \{r_i | r_i \in D(\pi_{d,l,i})\}$ – ресурсы АИС, ис-

пользуемые π_i протоколом, обеспечивающим функционирование сервиса d на уровне l модели OSI;

$R_{d,l,u} = \{r_i | r_i \in D(U_{d,l}), r_i \in R_{l,u}\}$ – ресур-

сы АИС, используемые АСУ для осуществления управляющих воздействий U на сервис d на уровне l модели OSI;

$R_{d,l,f} = \{r_i | r_i \in D(F_{d,l}), r_i \in R_{l,f}\}$ – ресур-

сы АИС, используемые системой ИТВ для осуществления воздействия F на сервис d на уровне l модели OSI;

$\Theta_{l,a} = \{(a_{l,i}, a_{l,j})\}$ – множество функциональных свя-

зей между алгоритмами A_i в протоколе π_i на уровне l модели OSI, где $i, j = 1 \dots |A|$;

t_0 – начальный момент функционирования АИС;

t_{B5} – текущий момент функционирования АИС;

$t_{=0l}$ – интервал времени наблюдения;

s_i – состояние протокола;

$S_{d,\theta} = \{s_{d,i}\} \cup \theta_{dl}$ – множество состояний прото-

колов и связей между ними на всех уровнях модели OSI, обеспечивающих функционирование сервиса d ;

$Z = \langle X, F, U \rangle$ – множество возможных значений внешних и внутренних воздействий на АИС (среда, ИТВ, УИВ и т.д.);

X – множество возможных значений факторов воздействий естественной среды на функционирование АИС;

F – множество возможных информационно-технических воздействий со стороны систем ИТВ;

U – множество управляющих воздействий на АИС со стороны АСУ;

Λ – информационная структура АИС, определяющая маршруты циркуляции информационных потоков;

$S_{conf} = \langle t_{тек}, R, \Omega, E, \Theta, Z, K, \Lambda \rangle$ – конфигу-

рация АИС, определяющая ее текущую структуру и множество функциональных связей;

$S_{conf}^{набл} =$

$= \{\langle t_{набл}, R, \Omega, E, \Theta, Z, K, \Lambda \rangle\} \in N$ – кон-

фигурация АИС, наблюдаемая со стороны АСУ;

$S_{conf}^{набл} =$

$= \{\langle t_{набл}, R, \Omega, E, \Theta, Z, K, \Lambda \rangle\} \in M$ – кон-

фигурация АИС, наблюдаемая со стороны системы ИТВ.

2) Параметры и показатели системы:

$Q = \langle T, Y, C, R, G \rangle$ – множество показателей качества функционирования АИС;

$E(\cdot)$ – область допустимых значений ($\cdot$);

q_i – отдельный показатель качества (QoS – Quality of Service) функционирования АИС;

$Q_{l,\pi,N} = \{q_i | q_i \in Q_{l,\pi}, q \in N_{l,\pi}\}$ – множество по-

казателей качества функционирования АИС, обеспечивающих работу протокола π_i на уровне l модели OSI и наблюдаемых системой управления АИС по каналу наблюдения N ;

$Q_{l,\pi,M} = \{q_i | q_i \in Q_{l,\pi}, q \in M_{l,\pi}\}$ – множество по-

казателей качества функционирования АИС, обеспечивающих работу протокола π_i на уровне l модели OSI и наблюдаемых системой ИТВ по каналу наблюдения M ;

$Q_{d,l,\pi} = \{q_i | q_i \in E(\pi_{d,l,i})\}$ – множество показа-

телей качества протокола π_i обеспечивающего функционирование сервиса d на уровне l модели OSI;

$Q_{d,l,\pi,N} = \{q_i | q_i \in Q_{d,l,\pi}, q \in N_{l,\pi}\}$ – множество

показателей качества, наблюдаемых АСУ по каналу наблюдения N , протокола π_i , обеспечивающего функционирование сервиса d на уровне l модели OSI;

$Q_{d,l,\pi,M} = \{q_i | q_i \in Q_{d,l,\pi}, q \in M_{l,\pi}\}$ – множе-

ство показателей качества, наблюдаемых системой ИТВ по каналу наблюдения M , протокола π_i , обеспечивающего функционирование сервиса d на уровне l модели OSI;

T_η – множество моментов времени наблюдения эле-

ментов АИС со стороны АСУ;

T_U – множество моментов времени выдачи управля-

ющих воздействий на элементы АИС со стороны АСУ;

T_F – интервал времени, в течение которого оказыва-

ются ИТВ на элементы АИС;

C – множество целей функционирования АИС;

C_0 – цель функционирования АИС;

$C_{много}$ – иерархическое представление целей АИС;

$G = \langle K_y, C_0, T_U \rangle$ – критерий способности АИС

выполнять целевую функцию, т.е. обеспечить непрерывное устойчивое функционирование АИС в киберпространстве;

K_y – обобщенный показатель устойчивости функционирования АИС в киберпространстве.

3) Связи внутри системы:

η_i – параметр, наблюдаемый со стороны системы управления АИС;

$N_{d,l,\pi} = \{\eta_i | \eta_i \in E(\pi_{d,l,i}), \eta_i \in \langle Q_{d,l,\pi}, Y_{d,l,\pi} \rangle\}$ – канал наблюдения АСУ выходных параметров Y и показателей качества функционирования Q протокола π_i обеспечивающего функционирование сервиса d на уровне l модели OSI;

μ_i – параметр, наблюдаемый со стороны системы ИТВ;

$M_{d,l,\pi} = \{\mu_i | \mu_i \in E(\pi_{d,l,i}), \mu_i \in \langle Q_{d,l,\pi}, Y_{d,l,\pi} \rangle\}$ – ка-

нал наблюдения системой ИТВ выходных параметров Y и показателей качества функционирования Q протокола π_i , обеспечивающего функционирование сервиса d на уровне l модели OSI;

$F_{d,l,\pi} = \{f_i | f_i \in D(\pi_{d,l,i}), f_i \in \langle R_{d,l,\pi}, \Omega_{d,l,\pi}, E_{d,l,\pi}, \Theta_{d,l,\pi} \rangle\}$ – множество

воздействий системы ИТВ на протоколы π_i , обеспечивающих функционирование сервиса d на уровне l модели OSI;

$\chi = \langle X, F, R \rangle$ – множество параметров

среды, определяющих параметрическое пространство АИС, с учетом ее ресурсов R , параметров естественной среды X и всего множества дестабилизирующих воздействий F на всех уровнях модели OSI;

$\chi_{d,l,\pi} = \langle X_{d,l,\pi}, F_{d,l,\pi}, R_{d,l,\pi} \rangle$ – множество параметров среды, определяющих параметрическое пространство протокола π_i обеспечивающего функционирование сервиса d с учетом необходимых ресурсов R , параметров естественной среды X и всего множества дестабилизирующих воздействий F на уровне l модели OSI;

$U_{d,l,\pi} = \{u_i | u_i \in D(\pi_{d,l,i})\}$ – множество управляющих воздействий АСУ с целью обеспечения требуемых показателей качества Q на протокол π_i обеспечивающий функционирование сервиса d на уровне l модели OSI;

y_i – выходной параметр АИС;
 $Y_{d,l,\pi} = \{y_i | y_i \in E(\pi_{d,l,i})\}$ – множество выход-

ных параметров протокола π_i обеспечивающего функционирование сервиса d на уровне l модели OSI;

$Y_{d,l,\pi,N} = \{y_i | y_i \in E(\pi_{d,l,i}), y_i \in N_{d,l,\pi}\}$ – мно-

жество выходных параметров, наблюдаемых АСУ по каналу наблюдения N , протокола π_i , обеспечивающего функционирование сервиса d на уровне l модели OSI;

$Y_{d,l,\pi,M} = \{y_i | y_i \in E(\pi_{d,l,i}), y_i \in M_{d,l,\pi}\}$ –

множество выходных параметров, наблюдаемых системой ИТВ по каналу наблюдения M , протокола π_i обеспечивающего функционирование сервиса d на уровне l модели OSI;

Ψ – отображение, задающее смену состояний АИС;

$\Psi_{d,l,\pi}$ – отображение, задающее смену состояний протокола π_i , обеспечивающего функционирование сервиса d на уровне l модели OSI;

$\Sigma_{d,l,\pi}$ – отображение, определяющее выходные показатели качества обслуживания Q протокола π_i , обеспечивающего функционирование сервиса d на уровне l модели OSI;

Υ – отображение, определяющее выходные параметры объекта АИС;

$\Upsilon_{d,l,\pi}$ – отображение, определяющее выходные параметры протокола π_i , обеспечивающего функционирование сервиса d на уровне l модели OSI;

Φ – отображение, определяющее параметрическое множество среды функционирования χ , зависящее от протоколов более высокого уровня $\Pi_{i,n+1}$ для протоколов всех уровней модели OSI;

$\Phi_{d,l,\pi}$ – отображение, определяющее параметрическое множество среды функционирования χ , зависящее от протоколов более высокого уровня $\pi_{i,l+1}$, i для протокола π_i , обеспечивающего работу сервиса d уровня l модели OSI;

Таким образом, разработанная модель АИС позволяет описать процесс функционирования и взаимосвязи как отдельных элементов (ИС, сетевые сервисы и ТСОИ), так и АИС в целом, как сложной иерархической организационно-технической системы, что позволяет перейти к рассмотрению непосредственно процесса обеспечения устойчивости функционирования АИС в киберпространстве и определению критериев оценки.

Процесс функционирования АИС в киберпространстве, как «агрессивной среде», связан с оказанием на ее элементы (ТСОИ, ИС) различных деструктивных воздействий (ИТВ), а основной задачей АСУ АИС является обеспечение устойчивости ее функционирования на основе адаптации внутреннего состояния системы к динамически изменяющейся внешней среде [3-5, 20].

Под устойчивостью АИС (АСУ СН), в соответствии с ГОСТ 34.003–90, понимается комплексное свойство системы, характеризующее живучестью, помехоустойчивостью и надежностью, а в соответствии с ГОСТ Р 53111–2018 под устойчивостью сетевых объектов понимается способность сети выполнять свои функции при выходе из строя части элементов сети в результате воздействия дестабилизирующих факторов.

Следовательно, основную задачу процесса обеспечения устойчивого функционирования АИС можно сформулировать следующим образом – создание условий для непрерывного функционирования АИС в

условиях воздействий агрессивной среды, а также восстановление своих характеристик при выходе из устойчивого состояния. Следовательно, тогда обобщенный показатель устойчивости функционирования АИС в киберпространстве имеет вид [9, 10]:

$$K_y = K_{\text{жив}} K_{\text{пом}} K_{\text{над}}, \quad (3)$$

где $K_{\text{жив}}$ – живучесть АИС в киберпространстве, трактуемая как вероятность сохранения АИС работоспособности (выживания) в условиях выхода из строя ее элементов, т. е. по сути отражает вклад каждого элемента АИС в выполнение ей целевой функции;

$K_{\text{пом}} = (1 - P_{\text{питв}}) (1 - P_{\text{пцтив}})$ – помехоустойчивость АИС в киберпространстве, трактуемая как вероятность выполнения АИС целевой функции с заданным качеством в условиях «общих» ($P_{\text{питв}}$) и целенаправленных ИТВ ($P_{\text{пцтив}}$);

$P_{\text{питв}}$ и $P_{\text{пцтив}}$ – вероятности поражения отдельных элементов ТСОИ и/или сервисов (ИС), входящих в АИС, «общими» и целенаправленными ИТВ, соответственно;

$K_{\text{над}}$ – надежность АИС в киберпространстве, трактуемая как вероятность обеспечения выполнения целевой функции АИС на протяжении определенного временного интервала в условиях возникновения различных событий ($i = 1, \dots, N$) – программных ошибок, технических сбоев и непреднамеренных ошибочных действий технического персонала и должностных лиц АИС, определяемая как:

$$K_{\text{над}} = \prod_{i=1}^N K_{\text{над}i} (1 - P_i) \quad (4)$$

где P_i – вероятность i -го события ($i = \overline{1, N}$).

Вследствие, довольно «жестким» требованиям, предъявляемым по технической надежности АИС, и предусмотренному ряду специальных мер по повышению оперативности устранения технических и программных отказов ТСОИ, вполне допустимо считать вероятность технических отказов элементов АИС при своевременном и качественном проведении технического обслуживания пренебрежительно малой.

Как следует из выражений (3) и (4), основой расчета устойчивости АИС является расчет его показателей помехоустойчивости и живучести. Причем определяющим свойством с точки зрения возможности выполнения АИС целевой функции будет живучесть, а помехозащищенность выступает ее составной частью.

В связи с тем, что свойства, характеризующие устойчивость АИС при осуществлении ИТВ (F), начинают проявляться только после того, как она подверглась воздействию, то мера живучести должна определяться условной вероятностью сохранения работоспособности при условии, что система получила локальное повреждение (Ω) [21, 22].

Под показателем живучести $K_{\text{жив}}$ будем понимать условную вероятность невыхода его конечного состояния за границы заданной области безопасных состояний S^1 пространства S в случае ИТВ:

$$K_{\text{жив}} = P[(\|S - s_0\| < S^1) / \Omega] \quad (5)$$

Исходя из понятия структурной уязвимости системы [8, 9], под которой будем понимать вероятность выхода конечного состояния системы из заданной безопасной области $S^1 - V_s$, справедливо соотношение:

$$K_{\text{жив}} = I - V_s, \quad (6)$$

а в конкретной точке на исследуемом временном интервале:

$$K_{\text{жив}}(t) = I - V_s(t). \quad (7)$$

Критерием для оценки живучести АИС будем считать выражение:

$$K_{\text{жив}}^{\text{тек}}(t) \geq K_{\text{АИС}}^{\text{тр}} \text{жив}(t), \quad (8)$$

где $K_{\text{АИС}}^{\text{тек}} \text{жив}(t)$ – текущий уровень живучести АИС, а $K_{\text{АИС}}^{\text{тр}} \text{жив}(t)$ – требуемый уровень его живучести в условиях осуществления ИТВ.

Используя выражения (5, 7, 8) и [21-23] определим следующий значения критерия способности АИС выполнять целевую функцию G в условиях ИТВ (рис. 3):

$$G = \begin{cases} K_{\text{АИС}}^{\text{тек}} \text{жив}(t) > 0,9 - \text{область оптимальных состояний;} \\ 0,9 \leq K_{\text{АИС}}^{\text{тек}} \text{жив}(t) < 0,7 - \text{область допустимых состояний;} \\ 0,7 \leq K_{\text{АИС}}^{\text{тек}} \text{жив}(t) < 0,5 - \text{область критических состояний;} \\ 0,5 \leq K_{\text{АИС}}^{\text{тек}} \text{жив}(t) < 0,3 - \text{граница областей крит./закрит. сост.;} \\ K_{\text{АИС}}^{\text{тек}} \text{жив}(t) \leq 0,3 - \text{область закритических состояний.} \end{cases} \quad (9)$$

Рис. 3. Схема соответствия класса состояния АИС уровню качества

Таким образом, в результате проведенного исследования осуществлена формализация процесса обеспечения устойчивости функционирования АИС в киберпространстве в условиях информационного противоборства, учитывающая сложный характер взаимодействия антагонистических систем, как внутри АИС, так и АИС со средой функционирования, и определены критерии оценки способности АИС выполнять целевую функцию в условиях ИТВ.

Выводы

По итогам представленных материалов статьи можно сделать следующие основные выводы.

Интеграция АИС через киберпространство порождает новые уязвимости и угрозы и ставит обеспечение национальной безопасности в зависимости от степени их защищенности. При этом под безопасностью АИС понимается состояние защищенности, обеспечивающее ее устойчивое функционирование в условиях «агрессивной среды». Очевидно, что для компенсации данных угроз необходимо внедрение соответствующей системы управления устойчивостью функционирования, которая будет рассматривать АИС как композицию вза-

имосвязанных функций, сетей и технологий, что определяет высокую сложность синтеза адекватной модели функционирования АИС в киберпространстве.

Применение системного подхода и соответствующих принципов к проведению исследований обеспечивает научность постановки и решения проблемы формализации процесса функционирования АИС в киберпространстве. Процесс синтеза данной модели выполнен путем перехода от общего к частному и агрегированием последовательности полученных результатов.

Элементом новизны разработанной модели процесса функционирования АИС в киберпространстве является представление АИС в виде сложной иерархической модели с описанием динамических процессов, учитывающей одноуровневые и разнуровневые функциональные отношения между элементами АИС (ИС, сетевыми сервисами, ТСОИ) и системами управления и ИТВ в соответствии с моделью OSI. Данные отношения рассматриваются в условиях информационного противоборства в киберпространстве с учетом показателей качества функционирования сетевых сервисов и ресурсов, необходимых для обеспечения устойчивого функционирования АИС.

К перспективным направлениям развития представленной в работе модели можно отнести следующее:

- исследование подсистем адаптивного мониторинга, способных осуществить синтез адекватной текущей ситуации модели объекта мониторинга в условиях динамических многосторонних конфликтов с различными типами конфликтного

взаимодействия (сотрудничество, нейтралитет, антагонистический конфликт);

- исследование АСУ, способных обеспечить устойчивость сложных многоуровневых систем в условиях динамических информационных конфликтов в киберпространстве.

Литература

1. Глобальная безопасность в цифровую эпоху: стратегии для России. Под общ. ред. Смирнова А.И. М.: ВНИИ геосистем, 2014. 394 с.
2. Стародубцев Ю.И., Бегаев А.Н., Давлятова М.А. Управление качеством информационных услуг / Под общ. ред. Ю.И. Стародубцева. СПб.: Изд-во Политехнического университета, 2017. 454 с.
3. Захарченко Р.И., Королев И.Д., Мирошниченко Е.Л. Противоборство в киберпространстве: концептуальные основы и терминологический базис // Научные труды КубГТУ, 2018, № 3. С.182-195.
4. Саенко И.Б., Ясинский С.А., Захарченко Р.И., Грязев А.Н. Модели и гипотезы информационного противоборства в кибернетическом пространстве // Информация и космос. 2018. №2. С.46–51.
5. Макаренко С.И. Информационное противоборство и радиоэлектронная борьба в сетевых войнах начала XXI века. Монография. – СПб.: Научно-технические технологии, 2017. 546 с.
6. Калинин В.Н., Резников Б.А. Теория систем и управления (структурно-математический подход). – Л.: ВИКИ, 1987. 417 с.
7. Щербатов И. А., Проталинский И. А. Сложные слабоформализуемые многокомпонентные технические системы // Управление большими системами: сборник статей. 2013. Вып. 45. С. 30-46.
8. Захарченко Р.И., Королев И.Д., Саенко И.Б. Синергетический подход к обеспечению устойчивости функционирования автоматизированных систем специального назначения // Системы управления, связи и безопасности. 2018. № 4. С. 207–225.
9. Минаев В.А., Королев И.Д., Зеленцова Е.В., Захарченко Р.И. Критическая информационная инфраструктура: оценка устойчивости функционирования // Радиопромышленность. 2018. Том №28, № 4. С. 59–67.
10. Минаев В.А., Крупенин А.В., Королев И.Д., Бондарь К.М., Захарченко Р.И. Оценка устойчивости функционирования критической информационной инфраструктуры федеральных органов исполнительной власти // Вестник Российского нового университета. Серия «Сложные системы: модели, анализ и управление». 2018. №4. С. 129-138.
11. Гуревич И.М. Многоуровневая модель сети связи // Вопросы кибернетики. Протоколы и методы коммутации в вычислительных сетях. 1986. Вып. 120. С. 72-88.
12. Абраменков А.Н., Петухова Н.В., Фархадов М.П., Фирсов А.В., Гуревич И.М. Многоуровневые модели сетевых систем и комплекс программ расчета их статических и динамических характеристик. XII Всероссийское совещание по проблемам управления ВСПУ-2014. 2014. С. 7375-7386.
13. Гуревич И.М. Динамическая модель сети связи // Теория телетрафика в системах информатики. 1989. С. 77-86.
14. Вакуленко А.А., Шевчук В.И. Математическая модель динамики конфликта радиоэлектронных систем // Радиотехника. 2011. № 1. С. 56-59.
15. Маевский Ю.И. Основные положения методологии синтеза многофункциональной конфликтно-устойчивой системы радиоэлектронной борьбы // Радиотехника. 2010. № 6. С. 61-66.
16. Паршуткин А.В. Концептуальная модель взаимодействия конфликтующих информационных и телекоммуникационных систем // Вопросы кибербезопасности. 2014. № 5 (8). С. 2-6.
17. Паршуткин А.В., Святкин С.А., Бажин Д.А., Сазыкин А.М. Радиоэлектронные информационные воздействия в конфликтах информационных и телекоммуникационных систем // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2015. № 5-6. С. 13-17.
18. Макаренко С.И. Динамическая модель двустороннего информационного конфликта с учетом возможностей сторон по наблюдению, захвату и блокировке ресурса // Системы управления, связи и безопасности. 2017. № 1. С. 60-97.
19. Макаренко С.И. Динамическая модель системы связи в условиях функционально-разноразного информационного конфликта наблюдения и подавления // Системы управления, связи и безопасности. 2015. № 3. С. 122-185.
20. Легков К.Е. Основные направления развития методологии управления сложными инфокоммуникационными системами специального назначения // Т-сomm: Телекоммуникации и транспорт. 2013. Т.7. №2. С. 41–46.
21. Махутов Н.А., Резников Д.О., Петров П.В., Куксова В.И. Оценка живучести сложных технических систем // Проблемы безопасности и чрезвычайных ситуаций. 2009. № 3. С. 47-66.
22. Казаков В. И. Основы теории топогеодезического обеспечения боевых действий войск. – М.: ВИА, 1977.
23. Probabilistic Modeling in System Engineering / Makhutov N.A. and etc., by ed. A. Kostogryzov. – London: IntechOpen, 2018. 278 p. DOI: 10.5772/intechopen.71396.

MODEL OF AUTOMATED INFORMATION SYSTEM OPERATION IN CYBERSPACE

Zakharchenko R.I.³, Korolev I.D.⁴

The purpose of the work is to formalize the process of special-purpose automated information system (AIS) operation in cyber space. At a time of information confrontation, the automated information system is considered as a complex multilevel hierarchical system, and its operation process is decomposed to separate network services and their supporting protocols by the levels of OSI model.

Methods used. The model has been developed using the methods of dynamical system theory, conflict theory, and theory of complex hierarchical systems.

Novelty. The element giving novelty to the developed model is representation of the automated information system in the form of a complex hierarchical model, which describes the dynamic processes, taking into account same-level and multilevel functional relationships between AIS elements (network services, information processing hardware) and AIS management systems, and information & technical influence in compliance with OSI model. Such relationships are considered in conditions of information confrontation in cyber space based on the operation quality parameters of network services and resources required to ensure operation and realization of both constructive and destructive impacts on network services.

Findings and their value. The developed model of AIS operation in cyber space can be used to elaborate new AIS management strategies considering the counteraction to information and technical influence in cyber space.

Keywords: model AIS, automated information system, information and technical impact, information conflict, model OSI.

References

1. Global'naya bezopasnost' v cifrovuyu ehposhu: stratagemy dlya Rossii. By ed. Smirnov A.I. Moscow, VNIIGeosystem, 2014, 394 p.
2. Starodubtsev Yu. I., Bugaev A. N., Davlyatova M. A. Upravlenie kachestvom informacionnyh uslug. By ed. Starodubtsev Yu. I. Saint-Petersburg, Publishing house of Polytechnic University, 2017, 454 p.
3. Zakharchenko R. I., Korolev I. D., Miroshnichenko E. L. Protivoborstvo v kiberprostranstve: konceptualnye osnovy i terminologicheskij bazis. Trudy V Mezhdunarodnoj NPK-2017. Krasnodar: Kuban State Technical University, 2017, pp. 112-131.
4. Saenko I.B., Yasinsky S.A., Zakharchenko R.I., Gryazev A.N. Modeli i gipotezy informacionnogo protivoborstva v kiberneticheskom prostranstve, Informaciya i kosmos [Information and space], 2018, No 2, pp.52-61.
5. Makarenko S. I. Informatsionnoe protivoborstvo i radioelektronnaya borba v setetsentricheskikh voynakh nachala XXI veka. Monografiya. Saint-Petersburg, Naukoemkie Tekhnologii, 2017, 546 p.
6. Kalinin V.N., Reznikov B.A. Teoriya sistem i upravleniya (strukturno-matematicheskij podhod). Leningrad, Viki, 1987, 417 p.
7. SCherbatov I. A., Protalinskij I. A. Slozhnye slaboformalizuemye mnogokomponentnye tekhnicheskie sistemy, Upravlenie bol'shimi sistemami: sbornik statej [Management of large systems: a collection of articles], 2013, No 45, pp. 30-46.
8. Zakharchenko R.I., Korolev I.D., Saenko I.B. Cinergeticheskij podhod k obespecheniyu ustojchivosti funkcionirovaniya avtomatizirovannyh sistem special'nogo naznacheniya, Sistemy upravleniya, svyazi i bezopasnosti [Control, communication and security systems], 2018, No 4, pp. 207-225.
9. Minaev V.A., Korolev I.D., Zelencova E.V., Zakharchenko R.I. Kriticheskaya informacionnaya infrastruktura: ocenka ustojchivosti funkcionirovaniya, Radiopromyshlennost' [Radio industry], 2018, Vol-28, No 4, pp. 59-67.
10. Minaev V.A., Krupenin A.V., Korolev I.D., Bondar' K.M., Zakharchenko R.I. Ocenka ustojchivosti funkcionirovaniya kriticheskoy informacionnoj infrastruktury federal'nyh organov ispolnitel'noj vlasti, Vestnik Rossijskogo novogo universiteta. Seriya «Slozhnye sistemy: modeli, analiz i upravlenie» [Bulletin of the Russian New University. Series "Complex systems: models, analysis and management"], 2018, No 4, pp. 129-138.
11. Gurevich I.M. Mnogourovnevaya model' seti svyazi. Voprosy kibernetiki. Protokoly i metody kommutacii v vychislitel'nyh setyah [Questions of cybernetics. Protocols and methods of switching in computer networks], 1986, No 120, pp. 72-88.
12. Abramnikov A.N., Petuhova N.V., Farhadov M.P., Frisov A.V., Gurevich I.M. Mnogourovnevye modeli setevykh sistem i kompleks programm rascheta ih staticheskikh i dinamicheskikh harakteristik. XII Vserossiyskoe soveshchanie po problemam upravleniya VSPU-2014. 2014, pp. 7375-7386.
13. Gurevich I.M. Dinamicheskaya model' seti svyazi. Teoriya teletrafika v sistemah informatiki [Teletraffic theory in computer systems], 1989, pp. 77-86.
14. Vakulenko A.A., Shevchuk V.I. Matematicheskaya model' dinamiki konflikta radioelektronnykh sistem, Radiotekhnika [Radiotechnics],

3 Roman Zakharchenko, Ph.D., Krasnodar Higher Military School, Krasnodar, Russia. E-mail: roman-zakharchenko@yandex.ru

4 Igor Korolev, Dr.Sc., Professor, Krasnodar Higher Military School, Krasnodar, Russia. E-mail: pi_korolev@mail.ru

- 2011, No 1, pp. 56-59.
15. Maevskij Yu.I. Osnovnye polozheniya metodologii sinteza mnogofunkcionalnoj konfliktno-ustojchivoj sistemy radioelektronnoj borby, Radiotekhnika [Radiotechnics], 2010, No 6, pp. 61-66.
 16. Parshutkin A.V. Konceptualnaya model' vzaimodejstviya konfliktuyushchih informacionnyh i telekommunikacionnyh system, Voprosy kiberbezopasnosti [Cybersecurity issues], 2014, No 5, pp. 2-6.
 17. Parshutkin A.V., Svyatkin S.A., Bazhin D.A., Sazykin A.M. Radioelektronnye informacionnye vozdejstviya v konfliktah informacionnyh i telekommunikacionnyh system, Voprosy oboronnoj tekhniki. Seriya 16: Tekhnicheskie sredstva protivodejstviya terrorizmu [Questions of defense engineering. Series 16: the technical means of combating terrorism], 2015, No 5-6, pp. 13-17.
 18. Makarenko S.I. Dinamicheskaya model dvunapravlenno informacionnogo konflikta s uchetom vozmozhnostej storon po nablyudeniyu, zahvatu i bloirovke resursa, Sistemy upravleniya, svyazi i bezopasnosti [System control, communication and security], 2017, No 1, pp. 60-97.
 19. Makarenko S.I. Dinamicheskaya model sistemy svyazi v usloviyah funkcionalno-raznouronovnogo informacionnogo konflikta nablyudeniya i podavleniya, Sistemy upravleniya, svyazi i bezopasnosti [System control, communication and security], 2015, No 3, pp. 122-185.
 20. Legkov K.E. Osnovnye napravleniya razvitiya metodologii upravleniya slozhnymi infokommunikacionnymi sistemami special'nogo naznacheniya, T-comm: Telekommunikacii i transport [T-comm: Telecommunications and transport], 2013, Vol-7, No 2, pp. 41-46.
 21. Mahutov N.A., Reznikov D.O., Petrov P.V., Kuksova V.I. Ocenka zhivuchesti slozhnyh tekhnicheskikh sistem, Problemy bezopasnosti i chrezvychajnyh situacij [Security and Emergency Issues], 2009, No 3, pp. 47-66.
 22. Kazakov V. I. Osnovy teorii topogeodezicheskogo obespecheniya boevyh dejstvij vojsk. Moscow, VIA, 1977.
 23. Probabilistic Modeling in System Engineering / Makhutov N.A. and etc., by ed. A. Kostogryzov. – London: IntechOpen, 2018. 278 p. DOI: 10.5772/intechopen.71396.