УДК 65.012.8

В.А. Мельник[1]
В.В. Завадский[2]
О.С. Деменко[3]

МОДЕЛЬ СИТУАЦИОННОГО УПРАВЛЕНИЯ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНЫХ СВЕДЕНИЙ ОБ ИННОВАЦИОННЫХ ОБРАЗЦАХ НА ЭТАПАХ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИХ И ОПЫТНО-КОНСТРУКТОРСКИХ РАБОТ

В работе предлагается ситуационный подход к моделированию процесса противодействия системы защиты конфиденциальных сведений и системы разведки конкурента при создании инновационных образцов.

Ключевые слова: *киберзащита, информационно-математический подход, информационные системы.*

V.A. Melnik
V.V. Zavadsky
O.S. Demenko

THE MODEL OF SITUATIONAL MANAGEMENT PROTECTION OF CONFIDENTIAL INFORMATION ON THE INNOVATION SAMPLES AT THE STAGES OF RESEARCH AND DEVELOPMENT WORKS

The paper proposes a situational approach to the modeling process of addressing system for the protection of sensitive information and systems intelligence of a competitor while creating innovative designs.

Keywords: *cyber defence, information and mathematical approach, information systems.*

Для применения ситуационного подхода к управлению системой защиты сведений конфиденциального характера (СЗКС) об инновационных образцах (ИО) на этапах научно-исследовательских и опытно-конструкторских работ (НИОКР) необходимо располагать знаниями о предметной области, которые позволят отразить смысловую взаимосвязь между элементами предметной области.

Анализ [2] показал, что для предоставления знаний, когда предметная область рассматривается как совокупность объектов и связывающих их отношений, целесообразно использовать сетевую модель знаний. В качестве носителя знаний в такой модели выступает семантическая сеть, вершины которой соответствуют объектам, а дуги – отношениям между объектами. В результате модель предметной области задается в виде двойки вида:

$$A_{по} = \{A, G\}, \quad (1)$$

где A – множество объектов предметной области; G – множество дуг, определяющих отношения между объектами предметной области.

В качестве объектов предметной области в СЗКС об ИО на этапах НИОКР включены:

– конкурент $A_{срк}$;
– СЗКС об ИО на этапах НИОКР $A_{сзкс}$;
– инновационный образец $A_{ио}$;
– информационное пространство $A_{ип}$.

Предметная область защиты конфиденциальных сведений об ИО на этапах НИОКР представлена на рис. 1.

Системой разведки конкурента $A_{срк}$ являются системы разведки иностранных государств, компаний и физических лиц – потребителей информации, которые предпринимают попытки сбора сведений, составляющих коммерческую тайну в Российской Федерации. Система разведки конкурента представляет собой совокупность сил $A^{c}_{срк}$, средств $A^{ср}_{срк}$ и способов $A^{сп}_{срк}$, предназначенных для сбора сведений, необходимых ЛПР $A_{срк} = \left\{ A^{c}_{срк}, A^{ср}_{срк}, A^{сп}_{срк} \right\}$. Состоит из:

– технической разведки;
– агентурной разведки;
– информационно-аналитической разведки.

[1] Кандидат технических наук, доцент ВА РВСН им. Петра Великого.

[2] Старший преподаватель АНО ВО «Российский новый университет».

[3] Слушатель ВА РВСН им. Петра Великого.

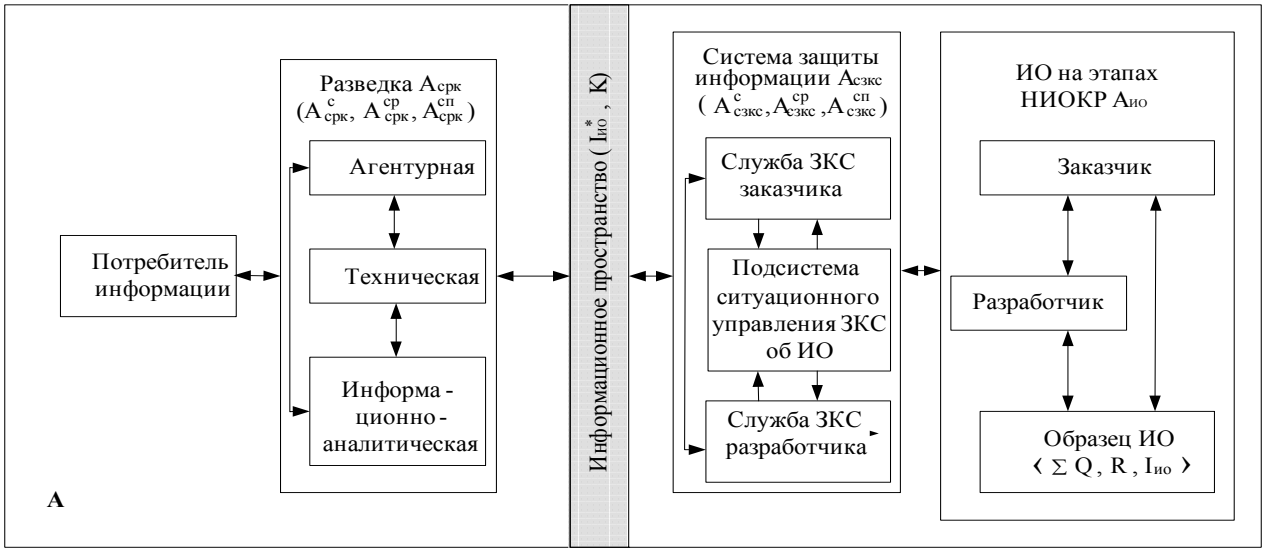

Рис. 1. Модель предметной области ЗС об ИО на этапах НИОКР

Под системой защиты сведений конфиденциального характера $A_{сзкс}$, согласно [5; 9], понимается совокупность органов защиты конфиденциальных сведений $A^{c}_{сзкс}$, используемых ими средств $A^{ср}_{сзкс}$ и способов защиты сведений $A^{сп}_{сзкс}$, составляющих конфиденциальных тайну, их носителей, а также мероприятий, проводимых в этих целях $A_{сзкс} = \left\{ A^{c}_{сзкс}, A^{ср}_{сзкс}, A^{сп}_{сзкс} \right\}$.

Инновационный образец $A_{ио}$ – создаваемый в интересах собственника образец, а также сведения о месте и процессе его создания, применяемых технологиях. Может быть как простой, так и сложной технической системой, состоящей из различных по своему составу и назначению подсистем и агрегатов. Инновационный образец может быть отображен кортежем, включающим наборы различных элементов (Σ), отношения между ними (R), свойства элементов (Q), а также множества сведений $I_{ио}$ о нем, которые имеют различную ценность и могут быть представлены в виде трёх его полноценных взаимосвязанных описаний: функционального $I^{ф}_{ио}$, информационного $I^{и}_{ио}$ и морфологического $I^{м}_{ио}$. Кроме этого образец характеризуется сопутствующей информацией $I^{с}_{ио}$, которая есть в большом количестве в открытом доступе, и за счет проведения информационно-аналитической работы позволяет получить это описание $A_{ио} = \left\{ \Sigma, R, Q, I_{ио} \right\}$.

Информационное пространство $A_{ип}$ не входит в область объектов $A_{срк}$ и $A_{сзкс}$, но обеспечивает взаимодействие объектов друг с другом, поэтому для рассматриваемой предметной области, согласно [6; 7], наибольший интерес представляют каналы K и уже имеющаяся информация об образце $I^{*}_{ио}$, содержащаяся в открытых источниках информационного пространства $A_{ип} = \left\{ K, I^{*}_{ио} \right\}$.

Согласно [6; 7; 13], общая ценность информации о разрабатываемом ИО определяется рядом показателей, среди которых основными являются оперативность их поступления, объем, простота представления и стоимость получения. При этом считается, что 90–95% знаний являются открытыми и несекретными.

В [6; 7; 8] показано, что подразделения информационно-аналитической разведки не считают главной задачей получение прямого доступа к защищаемым сведениям, а активно развивают способы получения таких сведений на основе анализа открытых источников, в которых могут содержаться сведения об ИО.

На основании вышеизложенного, для противодействия $A_{срк}$ СЗКС необходимо непрерывно осуществлять мониторинг открытых источников, собирать и анализировать сведения об ИО на этапах НИОКР, применять силы и средства, исходя из сложившейся ситуации [1; 12; 14], связанной с осведомлённостью конкурента.

В общем виде предметная область защиты сведений (ЗС) об ИО на этапах НИОКР A состоит из объектов

$$A = \left\{ A_{срк}, A_{сзкс}, A_{ио}, A_{ип} \right\}, \quad (2)$$

взаимосвязанных между собой.

Пусть отношение G_A – это взаимодействие между объектами (информационное, энергетическое, физическое и т.д.) предметной области, приводящее к изменению их характеристик и предметной области в целом. Тогда взаимодей-

ствие между объектами, входящими в предметную область A, может быть представлено в виде системы отношений G_A:

$$G_A=\begin{cases} G_{пр}\subset A_{сзкс}\times A_{ип}\times A_{срк} \\ G_{цл}\subset A_{срк}\times A_{ип}\times A_{ио} \\ G_{зщ}\subset A_{ио}\times A_{сзкс}\times A_{ип} \\ G_{ву}\subset A_{срк}\times A_{ип}\times A_{сзкс}\times A_{ио}\ , \end{cases} \qquad (3)$$

где $G_{пр}$ – отношения противодействия между $A_{срк}$ и $A_{сзкс}$, $G_{цл}$ – отношения целевого назначения применения $A_{срк}$, $G_{зщ}$ – отношения защиты , $A_{ио}-A_{сзкс}$, G_{by} – отношения формирования внешних условий.

В результате модель ситуационного управления ЗС об ИО на этапах НИОКР представлена на рис. 2

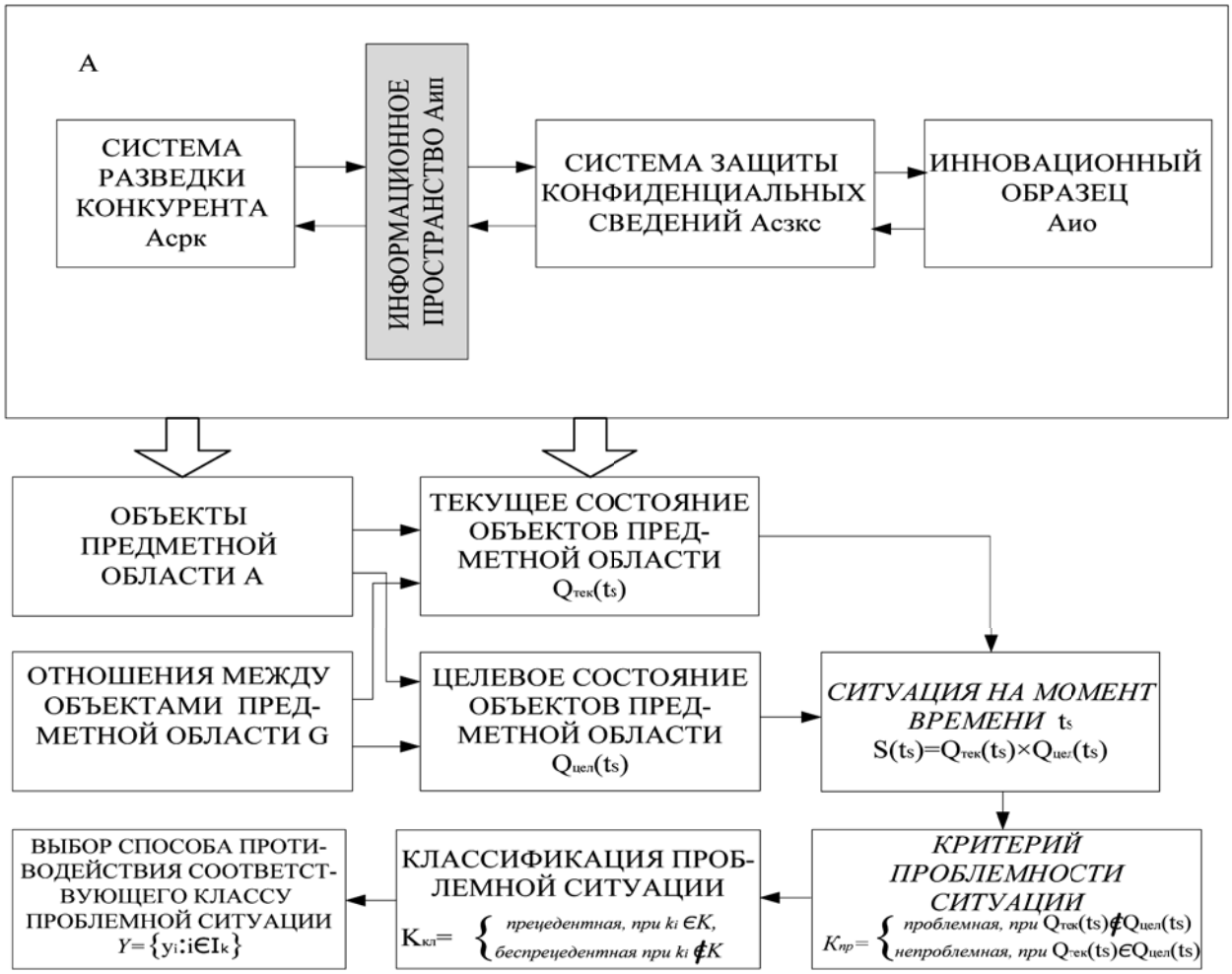

Рис. 2. Модель ситуационного управления ЗС об ИО на этапах НИОКР

Текущая ситуация $Q_{тек}$ в области защиты сведений об ИО на этапах НИОКР будет складываться на основании взаимодействия объектов предметной области A и отношений между ними G_A:

$$A\times G_A \to Q_{тек}. \qquad (4)$$

Если информация об $A_{ио}$ раскрывает защищаемые конфиденциальные сведения и не соответствует заданной на данный момент времени t пункту плана, а состояние системы управления и схема управления, определяемые полной ситуацией $S(t)$, допускают использование воздействия Y_k, то оно применяется, и текущая ситуация $Q_{тек}$ превращается в новую ситуацию $Q_{нов}$:

$$S:\ Q_{тек} \underset{Y_k}{\to} Q_{нов}. \qquad (5)$$

При проведении НИОКР по созданию ИО возникают различные ситуации, связанные с появлением в открытых источниках материалов, касающихся проводимых работ. В этих материа-

лах могут содержаться сведения как открытого, так и конфиденциального характера об ИО. СЗКС об ИО на этапах НИОКР должна провести оценку сложившейся ситуации и определить, к какой она относится. Проблемной считается такая ситуация, которая в соответствии с заранее разработанными ЛПР критериями (появление конфиденциальных сведений в открытом доступе) требует принятия управленческого решения. Непроблемная ситуация принятия решения не требует [4; 10; 11].

В сложившихся условиях, при выполнении мероприятий плана защиты конфиденциальных сведений об ИО на этапах НИОКР, СЗКС необходимо уделить особое внимание сведениям о ИО, циркулирующих в открытых источниках. В связи с многомерностью описания ИО на этапах НИОКР, для описания $\widetilde{I}_{uo}$ предлагается использовать нечеткую логику.

Описание объекта предметной области I_{uo} соответствует объекту $\widetilde{I}_{uo}$ [3] с неопределенными и фиксированными атрибутами и определяется как:

$$\widetilde{I}_{uoио}=\left\{x, \mu_{\widetilde{I}_{uo}}(x) \middle| x \in A_{uo}\right\}, \quad (6)$$

где $x-$ описание ИО или его элемента; $\mu_{\widetilde{I}_{uo}}(x)-$ функция принадлежности нечеткого множества $\widetilde{I}_{uo}$, A_{uo} – базовое множество.

Для оценки сложившейся ситуации в предметной области ЗС об ИО на этапах НИОКР введем коэффициент проблемности K_{np} защиты конфиденциальных сведений об ИО на этапах НИОКР в виде принадлежности сложившегося состояния системы Q_{mek} к требуемому Q_{mp}:

$$K_{np}=\begin{cases} проблемная, если\, Q_{тек} \notin Q_{mp} \\ непроблемная, если\, Q_{тек} \in Q_{mp}. \end{cases} \quad (7)$$

Если ситуация проблемная, определяем ее класс в соответствии с методикой классификации ситуаций в схеме принятия решений по противодействию получения информации об ИО на этапах НИОКР.

При проведении мероприятий по защите конфиденциальных сведений об ИО на этапах НИОКР система защиты конфиденциальных сведений $A_{сзкс}$ имеет ограниченное количество людских, материальных, финансовых, временных и информационных ресурсов, что обуславливает конечное множество применяемых ею способов $A^{сп}_{сзкс}$. Система разведки конкурента $A_{срк}$ также имеет ряд ограничений при выборе действий по сбору сведений, что также приводит к конечному множеству применяемых ею способов $A^{сп}_{срк}$.

Обозначим $A^{сп}_{сзкс}=\left\{A^{сп}_{сзксi} : i \in N_{сзкс}\right\}-$ множество способов применения сил и средств системы защиты конфиденциальных сведений об ИО на этапах НИОКР, $N_{сзкс}$ – число способов системы защиты конфиденциальных сведений; $A^{сп}_{срк}=\left\{A^{сп}_{сркj} : j \in N_{срк}\right\}-$ множество способов системы разведки конкурента по сбору информации, $N_{срк}$ – число способов системы разведки конкурента. В ходе противоборства каждая сторона будет стремиться выполнить свое предназначение путем реализации из множества стратегий той, которая бы обеспечила выполнение задач по предназначению.

В силу конечности числа различных воздействий все множество возможных ситуаций раскладывается на $k_i \in K$ классов, каждому из которых будет соответствовать одно или несколько возможных воздействий $Y_k \in A^{сп}_{сзксi}$.

Если выбранный способ привел к желаемому результату и система вернулась к требуемому состоянию, дальнейшее вмешательство в работу не требуется. Если ситуация осталась проблемной, проводится ее классификация и выбирается новый способ из имеющегося в наличии. Если проблему не удается устранить, необходимо пересмотреть цели плана мероприятий ЗС об ИО на этапах НИОКР.

Таким образом, предложенная модель ситуационного управления позволит оперативно принимать решения и рационально применять силы и средства СЗКС об ИО на этапах НИОКР при возникновении проблемных ситуаций.

Литература

1. Поспелов Д.А. Ситуационное управление: теория и практика. – М. : Наука, 1986. – 288 с.

2. Болотова Л.С. Системы искусственного интеллекта: модели и технологии, основанные на знаниях. – М. : Финансы и статистика, 2012. – 664 с.

3. Мелихов А.Н., Берштейн Л.С., Коровин С.Я. Ситуационные советующие системы с нечеткой логикой. – М. : Наука. – Гл. ред. физ.-мат.лит., 1990. – 272 с.

4. Потюпкин А.А. Диссертация кандидата технических наук : 20.02.12. Инв. № 137445, 2014. – 190 с.

5. Указ Президента РФ от 06.03.1997 г. № 188 «Об утверждении сведений конфиденциального характера» (в редакции от 13.07.2015 г.).

6. Духидин В.В., Духидина О.В. Конкурентная разведка в Internet. Советы аналитика. – М. : ДМК Пресс, 2002. – 192 с.

7. Блюмин А.М., Феоктистов Н.А. Мировые информационные ресурсы. – М. : ИТК Дашков и К°, 2001. – 296 с.

8. Гладышев А.И. Разработка имитационной модели вирусной эпидемии на основе модели биологических вирусов: принципы, основные параметры, описание и зависимости // Вестник Российского нового университета. – 2012. – Выпуск 4. Управление, вычислительная техника и информатика.

9. Гладышев А.И., Жуков А.О. Использование в автоматизированной системе контроля полномочий биометрической идентификации // Вестник Российского нового университета. – 2013. – Выпуск 4. Управление, вычислительная техника и информатика.

10. Гладышев А.И. Удобство и безопасность компьютерных систем, в чем противоречие? // Вестник Российского нового университета. – 2012. – Выпуск 4. Управление, вычислительная техника и информатика.

11. Гладышев А.И., Жуков А.О. Достоинства и недостатки имитационного моделирования с использованием нейронных сетей // Вестник Российского нового университета. – 2013. – Выпуск 4. Управление, вычислительная техника и информатика.

12. Гладышев А.И., Жуков А.О. Методика использования искусственных нейронных сетей с целью идентификации параметров движения летательных аппаратов // Вестник Российского нового университета. – 2014. – Выпуск 4. Управление, вычислительная техника и информатика.

13. Гладышев А.И. Вопросы создания единого информационного пространства в космотехносфере // Вестник Российского нового университета. – 2014. – Выпуск 4. Управление, вычислительная техника и информатика.

14. Гладышев А.И. Анализ системы управления сложными динамическими объектами (системами) // Вестник Российского нового университета. Серия «Сложные системы: модели, анализ и управление». – 2015. – Выпуск 1.