УДК 004.8

Системный подход к проектированию интеллектуальных систем защиты информации*

[1] Симон Жоржевич Симаворян
[2] Арсен Рафикович Симонян
[3] Улитина Елена Ивановна
[4] Рафик Арсенович Симонян

[1] Сочинский государственный университет, Российская Федерация
354000, г. Сочи, Краснодарский край, ул. Советская, 26а
Кандидат технических наук, доцент
E-mail: simsim58@mail.ru
[2] Сочинский государственный университет, Российская Федерация
354000, г. Сочи, Краснодарский край, ул. Советская, 26а
кандидат физико-математических наук, доцент
E-mail: oppm@mail.ru
[3] Сочинский государственный университет, Российская Федерация
354000, г. Сочи, Краснодарский край, ул. Советская, 26а
кандидат физико-математических наук, доцент
E-mail: ulitinaelena@mail.ru
[4] Кубанский государственный университет, Российская Федерация
350040, г. Краснодар, , ул. Ставропольская, 149
Аспирант
E-mail: raf55@list.ru

Аннотация. В данной статье сделана попытка формирования основ теории интеллектуальной защиты информации в автоматизированных системах обработки информации на основе системно-концептуального подхода и кратко изложен системный подход к проектированию интеллектуальных систем защиты информации.

Ключевые слова: интеллектуальные системы защиты информации; системный подход.

Введение. Применительно к проблеме проектирования интеллектуальных систем защиты информации необходимо отметить, что в основу методологии формирования теории интеллектуальной защиты информации необходимо положить так называемый системно-концептуальный подход к защите информации [1] и теории интеллектуальных информационных систем в области искусственного интеллекта [3]. Сущность системного подхода заключается в трех посылках [1]: 1) системное рассмотрение сущности исследуемой проблемы; 2) разработка и обоснование полной и непротиворечивой концепции решения проблемы; 3) системное использование методов моделирования исследуемых (разрабатываемых) процессов и явлений.

Постановка задачи. Данная статья является первой попыткой формирования основ теории интеллектуальной защиты информации в автоматизированных системах обработки информации (АСОД) на основе вышеприведенных подходов. Поэтому она и должна рассматриваться лишь как первое приближение к формированию полной и непротиворечивой теории.

Обсуждение. Под концепцией защиты информации понимается полная совокупность взглядов, положений и решений, необходимых и достаточных для целенаправленного и оптимального решения всех задач теоретических исследований и практической реализации проблем защиты информации в современных АСОД [1, 2]. Система требований к формированию концепции защиты информации сформулирована в [1, 2]:

* Работа поддержана грантом РФФИ 13-01-00544.

1) Общетеоретические требования: а) полнота, т.е. достаточность для решения всех задач анализа и синтеза систем защиты и управления их функционированием; б) непротиворечивость, т.е. взаимосвязанность и логическая стройность всех её компонентов; в) стройность, т.е. соответствие понятию научного дизайна;

2) прикладные требования: а) унифицированность, т.е. способность обеспечивать потребности решения задач комплексной защиты информации; б) учет всех основных положений современных и перспективных концепций построения и использования АСОД; в) реализуемость, т.е. возможность реализации при современном состоянии науки, техники и производства; г) перспективность, т.е. адекватность не только для нынешних, но и будущих потребностей и условий защиты информации в автоматизированных системах. Общая структура системной концепции защиты информации приводится в [1,2].

Искусственный интеллект (ИИ) как наука существует около полувека. Интеллектуальные информационные системы проникают во все сферы нашей жизни, например, в такие как: 1) разработка интеллектуальных информационных систем или систем, основанных на знаниях; 2) разработка естественно-языковых интерфейсов и машинный перевод; 3) генерация и распознавание речи; 4) обработка визуальной информации; 5) обучение и самообучение; 6) распознавание образов; 7) игры и машинное творчество; 8) программное обеспечение систем ИИ; 8) новые архитектуры компьютеров; 9) интеллектуальные роботы [3].

Интеллектуальные информационные системы (ИС) основаны на концепции использования базы знаний для генерации алгоритмов решения прикладных задач различных классов в зависимости от конкретных информационных потребностей пользователей [3, 9, 10].

Для интеллектуальной ИС характерны следующие признаки [3, 11]:

- развитые коммуникативные способности;
- умение решать сложные плохо формализуемые задачи;
- способность к самообучению;
- адаптивность.

Каждому из перечисленных признаков условно соответствует свой класс интеллектуальных ИС. Различные системы могут обладать одним или несколькими признаками интеллектуальности с различной степенью проявления.

Средства ИИ могут использоваться для реализации различных функций, выполняемых интеллектуальными ИС. Интеллектуальным ИС присущи следующие интеллектуальные функции:

- коммуникативные способности - способ взаимодействия конечного пользователя с системой;
- решение сложных плохо формализуемых задач, которые требуют построения оригинального алгоритма решения в зависимости от конкретной ситуации, характеризующейся неопределенностью и динамичностью исходных данных и знаний;
- способность к самообучению – умение системы автоматически извлекать знания из накопленного опыта и применять их для решения задач;
- адаптивность – способность системы к развитию в соответствии с объективными изменениями области знаний.

Общая структура унифицированной концепции интеллектуальной защиты информации приводится на рис.1, из которого следует, что исходную основу концепции интеллектуальной защиты составляют: 1) концепции построения интеллектуальных АСОД, 2) концепции построения интеллектуальных баз данных и технологий обработки информации, 3) условия функционирования. К параметрам защиты информации относятся: 1) объекты и элементы защиты информации с учетом их интеллектуализации;

2) уровни интеллектуальной защиты информации и требования к ним;

3) показатели защищенности информации.

Очень важным компонентом концепции является понятие интеллектуального множества каналов несанкционированного получения информации, базирующее на таком понятии как интеллектуальные злоумышленные действия [6, 7, 8]. Для обеспечения возможностей практической реализации концепции использования знаний о злоумышленных действиях с целью построения интеллектуальных баз данных и технологий

обработки информации должна быть разработана методология оценки интеллектуальной защищенности информации [4, 5, 7].

Конструктивными элементами концепции являются: 1) интеллектуальные функции защиты информации, 2) интеллектуальные задачи защиты информации, 3) интеллектуальные средства защиты информации, 4) интеллектуальная система защиты информации, 5) механизмы обеспечения функционирования интеллектуальной системой защиты информации, 6) механизмы управления интеллектуальной системой защиты информации.

Важнейшим элементом концепции является обратная связь от конструктивных элементов концепции к элементам составляющим исходную основу концепции.

Интеллектуальная функция защиты информации – совокупность однородных в функциональном отношении интеллектуальных мероприятий, регулярно осуществляемых в АСОД, с целью создания, поддержания и обеспечения условий, объективно необходимых для надежной защиты информации. Интеллектуальная задача защиты информации – интеллектуальные организованные возможности, интеллектуальных средств, методов и мероприятий, реализуемых в АСОД с целью реализации интеллектуальных средств защиты информации.

Интеллектуальное средство защиты информации – интеллектуальные устройства, программы и мероприятия, специально предназначенные для решения в АСОД интеллектуальных задач защиты информации. Интеллектуальная система защиты информации – организованная совокупность всех интеллектуальных средств, методов и мероприятий, предусматриваемых в АСОД с целью осуществления интеллектуальной защиты информации.

Разработка и обоснование основных положений концепции интеллектуальной защиты информации составляет основное содержание проекта 13-01-00544 – « Интеллектуальные системы защиты информации».

<table>
<tr><td colspan="5">Условия, способствующие повышению эффективности интеллектуальной защиты информации</td></tr>
<tr><td>ИСХОДНАЯ ОСНОВА</td><td>ПАРАМЕТРЫ ЗАЩИТЫ ИНФОРМАЦИИ</td><td>СИСТЕМА ДЕСТАБИЛИЗИРУЮЩИХ ФАКТОРОВ</td><td>ПАРАМЕТРЫ ЗАЩИЩЕННОСТИ</td><td>КОНСТРУКТИВНЫЕ ЭЛЕМЕНТЫ</td></tr>
<tr><td rowspan="2">Концепции построения интеллектуальных АСОД</td><td rowspan="2">Объекты и элементы защиты с учетом возможности их интеллектуализации</td><td rowspan="5">Интеллектуальное множество КНПИ</td><td rowspan="5">Методика оценки интеллектуальной защищенности информации</td><td>Механизмы управления интеллектуальной системой защиты</td></tr>
<tr><td>Механизмы обеспечения функционирования интеллектуальной системой</td></tr>
<tr><td>Концепции построения интеллектуальных баз данных и технологий обработки информации</td><td>Уровни интеллектуальной защиты и требования к ним</td><td>Интеллектуальная система защиты информации</td></tr>
<tr><td rowspan="2">Условия функционирования АСОД</td><td rowspan="2">Показатели интеллектуальной защищенности информации</td><td>Интеллектуальные функции защиты информации</td></tr>
<tr><td>Интеллектуальные задачи защиты информации</td></tr>
<tr><td></td><td></td><td></td><td></td><td>Интеллектуальные</td></tr>
</table>

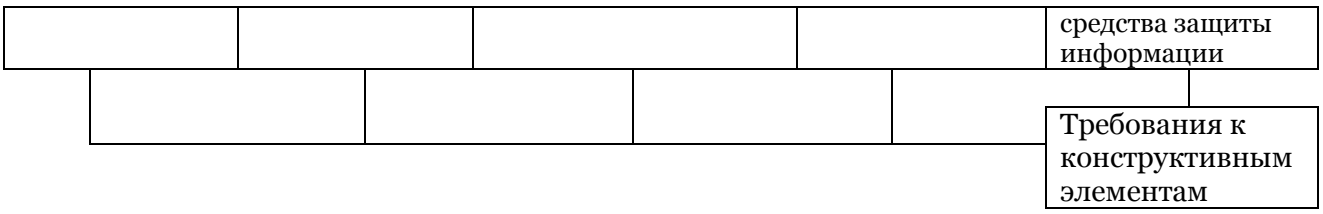

Рис. 1. Общая структура унифицированной концепции защиты информации

Материалы и методы. В работе использованы достижения системно-концептуального подхода к защите информации [1] и теория интеллектуальных информационных систем в области искусственного интеллекта [3].

Результаты. В работе кратко приведены результаты решения задачи «Разработка концепции построения интеллектуальной системы защиты информации на основе системного подхода» в рамках гранта РФФИ 13-01-00544.

Выводы. Нетрудно видеть, что перечисленные элементы концепции составляют логически стройную, полную и непротиворечивую последовательность решений, реализация которых создает предпосылки для разработки надежной интеллектуальной системы защиты информации.

Примечания.

1. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2-х кн.: М.: Энергоатомиздат, 1994.

2. Герасименко В.А., Малюк А.А. Основы защиты информации. Учебник: М.: Известия. 1997.

3. Тельнов Ю.Ф. Интеллектуальные информационные системы. (Учебное пособие) М., 2000.

4. Симаворян С.Ж. Понятие неопределенности в задачах защиты информации. Обозрение прикладной и промышленной математики, том 16, выпуск 6. Ред. Ю.В. Прохоров. М.:ООО Редакция журнала «ОПиПМ», 2009, с. 1115.

5. Симаворян С.Ж. Аналитическая модель определения показателя уязвимости информации в автоматизированных системах обработки информации (АСОД). Обозрение прикладной и промышленной математики, том 16, выпуск 6. Ред. Ю.В. Прохоров. М.: ООО Редакция журнала «ОПиПМ», 2009, с. 1114.

6. Симаворян С.Ж. Применение методов Data Mining для обнаружения инсайдеров. Обозрение прикладной и промышленной математики, том 17, выпуск 3. Ред. Ю.В. Прохоров. М.:ООО Редакция журнала «ОПиПМ», 2011, С. 455-456.

7. Simon Zh. Simavoryan, Arsen R. Simonyan. The Probabilistic Safety Assessment Model of Anti-Terrorist Security of Olympic games. European Researcher, 2012, Vol(20), № 5-1, pp. 532-536.

8. Дунин В.С., Хохлов Н.С. Модель угроз информационной безопасности комплексной автоматизированной интеллектуальной системы «безопасный город». //Вестник Воронежского института МВД России. 2011. № 4. С. 74-79.

9. Трегубов А.Г. Построение интеллектуальных комплексов защиты информации в автоматизированных системах. // Проблемы информационной безопасности. Компьютерные системы. 2007. № 1. С. 7-10.

10. Нестерук Ф.Г. К организации интеллектуальной защиты информации. // Труды СПИРАН. 2009. № 10. С. 148-159.

11. Макаров И.М., Лохин В.М., Манько С.В., Романов М.П. Искусственный интеллект и интеллектуальные системы управления. Наука, 2006, 336 с.

UDC 004.8

Systematic Approach to Designing Intelligent Information Security Systems

[1] Simon Zh. Simavoryan
[2] Arsen R. Simonyan

[3] Elena I. Ulitina
[4] Rafik A. Simonyan

[1] Sochi State University, Russian Federation
354000 Sochi, 26a Sovetskaya St.
PhD (Technical), Associate professor
E-mail: simsim58@mail.ru
[2] Sochi State University, Russian Federation
354000 Sochi, 26a Sovetskaya St.
PhD (Physics and mathematical), Associate professor
E-mail: oppm@mail.ru
[3] Sochi State University, Russian Federation
354000 Sochi, 26a Sovetskaya St.
PhD (Physics and mathematical), Associate professor
E-mail: elenaulitina@mail.ru
[4] Kuban State University, Russian Federation
350040 Krasnodar, Stavropolskaya St., 149
E-mail: raf55@list.ru
Post-graduate student

Abstract. The present article attempts to create the basis for a theory of the intelligent protection of information within automated information processing systems on the basis of a systematic conceptual approach and briefly outlines the systematic approach to designing intelligent information security systems.

Keywords: intelligent information security systems; systematic approach.