www.volsu.ru

DOI: https://doi.org/10.15688/NBIT.jvolsu.2019.1.2

УДК 004:002
ББК 32.97

ОСНОВЫ ОРГАНИЗАЦИИ АДАПТИВНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Анастасия Олеговна Калита

Преподаватель кафедры информационной безопасности,
Севастопольский государственный университет
aokalita@sevsu.ru
ул. Курчатова, 7, 299015 г. Севастополь, Российская Федерация

Марина Ивановна Ожиганова

Кандидат технических наук, доцент,
заведующий кафедрой информационной безопасности,
Севастопольский государственный университет
m.i.ozhiganova@sevsu.ru
ул. Курчатова, 7, 299015 г. Севастополь, Российская Федерация

Евгений Николаевич Тищенко

Доктор экономических наук, профессор,
заведующий кафедрой информационных технологий и защиты информации,
Ростовский государственный экономический университет
celt@inbox.ru
ул. Большая Садовая, 69, 344002 г. Ростов-на-Дону, Российская Федерация

Аннотация. В данной статье рассматриваются общие принципы построения адаптивных систем. Также исследованы существующие подходы к организации адаптивных систем защиты информации.

Ключевые слова: информационная безопасность, адаптивные системы защиты информации, биосистемная адаптация, типовая модель адаптивной системы защиты информации, организация систем защиты информации.

На протяжении последних нескольких десятков лет наблюдается тенденция минимизации участия человеческого фактора в различных производственных (и не только) процессах. Данный процесс реализуется посредством массового внедрения автоматизированных систем (далее – АС). Человеко-машинные комплексы на данный момент являются наиболее распространенной и продуктивной моделью осуществления деятельности.

На текущем этапе развития технологий процесс автоматизации человеческой деятельности представляет собой только промежуточное звено на пути к исключению человеческого вмешательства. Данное направление наиболее актуально для систем, которые несут потенциальную и реальную угрозу здо-

ровью и жизни человека (например, заводы обрабатывающей промышленности) или системы, угрозой которым является человек (например, транспортные системы). Ко второй группе можно отнести сферу информационной безопасности. Существует необходимость в переходе на следующий уровень исключения человеческого фактора – внедрение адаптивных систем, которые позволят перенести процесс защиты информации в совершенно иную плоскость.

Организация адаптивных систем защиты информации строится на применении существующих методов адаптации из других областей научного знания в отношении вопросов информационной безопасности. Особенности такого прикладного применения обобщенных принципов адаптации отражают специфику предметной области, не нарушая общепринятых норм.

Так, принципы организации адаптивных систем защиты информации должны основываться на модели адаптации систем управления. Рассматриваются два основных вида адаптации:

– параметрическая: коррекция, подстройка параметров систем без изменения принципов работы системы;

– структурная адаптация: адаптация структуры модели, допускающая сохранение значений параметров системы [6].

Помимо классификации, необходимо рассмотреть обобщенный алгоритм построения моделей адаптированных систем. Так, в общем виде, он содержит следующие этапы:

1. Исследование методов и моделей адаптации, для поиска удовлетворяющих требования разрабатываемой системы.

2. Модификация выбранных методов и моделей для корректного функционирования в рамках текущей области применения.

3. Апробация внедрения адаптированных принципов по отношению к разрабатываемой системе и проверка на соответствие итогов планируемым результатам.

Вопрос применения принципов адаптивного управления в области информационной безопасности выдвигается не впервые. Существуют как типовые модели адаптивной системы защиты информации (далее – СЗИ), так и прикладные модели, учитывающие особенности конкретных областей защиты информации.

При исследовании существующих моделей адаптивных СЗИ, следует начать с рассмотрения типовой адаптивной СЗИ (рис. 1) [4].

Как видно из типовой модели, приведённой на рисунке 1, системы адаптивной ЗИ могут основываться на структурной адаптации. Данная модель отражает общий подход к функционированию СЗИ с адаптивным управлением без учета особенностей подсистем защиты информации.

Обобщенная архитектура адаптивного самообучающегося средства защиты информации приведена на рисунке 2 [1].

Основная область применения адаптивных СЗИ – обеспечение информационной безопасности в информационных технологиях

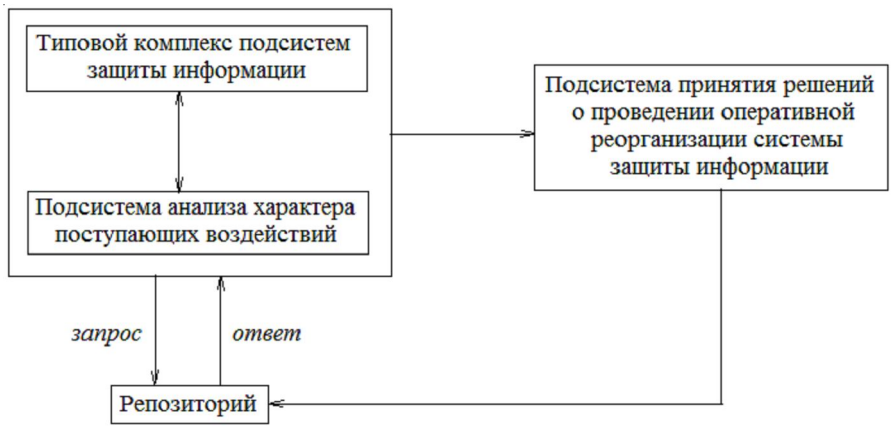

Рис. 1. Типовая адаптивная СЗИ

(далее – ИТ). Такие системы строятся на биосистемных аналогиях между эволюцией биосистем и систем информационных технологий. В качестве перспективного метода разработки систем информационной безопасности (далее – ИБ) рассматривается использование подобия механизмов защиты информационных процессов биосистем в искусственных системах [3].

Биосистемная аналогия систем информационных технологий представлена на рисунке 3 [3].

Принцип биосистемной адаптации, аналогично иерархии системы защиты информационных процессов и ресурсов в биологических системах, обеспечивается на двух уровнях:

– нижний уровень – механизмы иммунной системы;

– верхний уровень – механизмы адаптивной памяти и накопления жизненного опыта [5].

При использовании биологических механизмов в компьютерных системах следует придерживаться следующих этапов:

– нахождение методов и структур, имеющих аналогию как в биологических, так и в компьютерных системах;

– описание и построение модели поведения биосистемы;

– непосредственное использование биологических аналогий в компьютерных системах [2].

Такой подход также можно использовать для внедрения биосистемных принципов в системах защиты информации, заменив таким образом «компьютерные системы» на более обобщенное понятие «информационные системы».

СПИСОК ЛИТЕРАТУРЫ

1. Жуков, В. Г. Применение нечетких искусственных иммунных систем в задаче построения адаптивных самообучающихся средств защиты информации / В. Г. Жуков, М. Н. Жукова, Н. А. Коромыслов // Сибирский журнал науки и технологий. – 2012. – № 1 (41). – Электрон. текстовые дан. – Режим доступа: https://cyberleninka.ru/article/n/primenenie-nechetkih-iskusstvennyh-immunnyh-sistem-v-zadache-postroeniya-adaptivnyh-samoobuchayuschihsya-sredstv-zaschity (дата обращения: 15.04.2019). – Загл. с экрана.

2. Котенко, И. В. Анализ биоинспирированных подходов для защиты компьютерных систем и сетей / И. В. Котенко, А. В. Шоров, Ф. Г. Нестерук // Труды СПИИРАН. – 2011. – № 3 (18). – Электрон. текстовые дан. – Режим доступа: http://www.mathnet.ru/links/6dd22b2a6595ceea5c900fbc547fd9f5/trspy450.pdf (дата обращения: 20.04.2019). – Загл. с экрана.

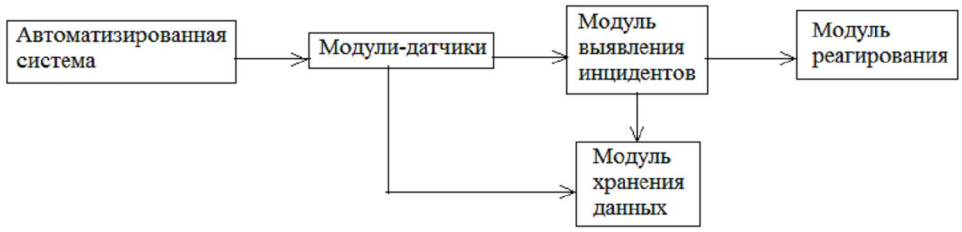

Рис. 2. Архитектура адаптивного самообучающегося средства ЗИ

Рис. 3. Биосистемная аналогия ИТ-систем

3. К разработке модели адаптивной защиты информации / Ф. Г. Нестерук, Л. Г. Осовецкий, Г. Ф. Нестерук, Р. Ш. Фахрутдинов // Специальная техника. – 2005. – № 2. – Электрон. текстовые дан. – Режим доступа: https://elibrary.ru/download/elibrary_17103979_48622109.pdf (дата обращения: 20.04.2019). – Загл. с экрана.

4. Левкин, И. М. Типовая структура и состав адаптивной системы защиты информации большой информационной систем / И. М. Левкин, А. А. Володина. – Электрон. текстовые дан. – Режим доступа: http://ubs.mtas.ru/bitrix/components/bitrix/forum.interface/show_file.php?fid=16693 (дата обращения: 15.04.2019). – Загл. с экрана.

5. Нестерук, Ф. Г. К организации интеллектуальной защиты информации / Ф. Г. Нестерук // Труды СПИИРАН. – 2009. – № 10. – Электрон. текстовые дан. – Режим доступа: https://elibrary.ru/download/elibrary_15512718_45029580.pdf (дата обращения: 18.04.2019). – Загл. с экрана.

6. Растригин, Л. А. Адаптация сложных систем / Л. А. Растригин. – Рига : Зинатне, 1981. – 375 с.

REFERENCES

1. Zhukov V.G., Zhukova M.N., Koromyslov N.A. Primenenie nechetkikh iskusstvennykh immunnykh sistem v zadache postroeniya adaptivnykh samoobuchayushchikhsya sredstv zashchity informatsii [Application of Fuzzy Artificial Immune Systems in the Task of Building Adaptive Self-Learning Means of Information Protection]. *Sibirskiy zhurnal nauki i tekhnologiy* [Siberian Journal of Science and Technology], 2012, no. 1 (41). URL: https://cyberleninka.ru/article/n/primenenie-nechetkih-iskusstvennyh-immunnyh-sistem-v-zadache-postroeniya-adaptivnyh-samoobuchayuschihsya-sredstv-zaschity (accessed 15 April 2019).

2. Kotenko I.V., Shorov A.V., Nesteruk F.G. Analiz bioinspirirovannykh podkhodov dlya zashchity kompyuternykh sistem i setey [Analysis of Bioinspired Approaches for Protection of Computer Systems and Networks]. *Trudy SPIIRAN* [SPIIRAS Proceedings], 2011, no. 3 (18). URL: http://www.mathnet.ru/links/6dd22b2a6595ceea5c900fbc547fd9f5/trspy450.pdf (accessed 20 April 2019).

3. Nesteruk F.G., Osovetskiy L.G., Nesteruk G.F., Fakhrutdinov R.Sh. K razrabotke modeli adaptivnoy zashchity informatsii [To Develop a Model of Adaptive Information Security]. *Spetsialnaya tekhnika*. 2005. no. 2. URL: https://elibrary.ru/download/elibrary_17103979_48622109.pdf (accessed 20 April 2019).

4. Levkin I.M., Volodina A.A. *Tipovaya struktura i sostav adaptivnoy sistemy zashchity informatsii bolshoy informatsionnoy sistem* [Typical Structure and Composition of Adaptive Information Security System of Large Information System]. URL: http://ubs.mtas.ru/bitrix/components/bitrix/forum.interface/show_file.php?fid=16693 (accessed 15 April 2019).

5. Nesteruk F.G. K organizatsii intellektualnoy zashchity informatsii [To the Organization of Intellectual Information Protection]. *Trudy SPIIRAN* [SPIIRAS Proceedings], 2009, no. 10. URL: https://elibrary.ru/download/elibrary_15512718_45029580.pdf (accessed 18 April 2019).

6. Rastrigin L.A. *Adaptatsiya slozhnykh sistem* [Adaptation of Complex Systems]. Riga, Zinatne Publ., 1981. 375 p.

BASICS OF ADAPTIVE INFORMATION SECURITY SYSTEMS

Anastasia O. Kalita

Lecturer, Department of Information Security,
Sevastopol State University
aokalita@sevsu.ru
Kurchatova St., 7, 299015 Sevastopol, Russian Federation

Marina I. Ozhiganova

Candidate of Sciences (Engineering), Associate Professor,
Head of the Department of Information Security,
Sevastopol State University
m.i.ozhiganova@sevsu.ru
Kurchatova St., 7, 299015 Sevastopol, Russian Federation

Evgeny N. Tishchenko

Doctor of Sciences (Economics), Professor,
Head of the Department of Information Technology and Information Protection,
Rostov State Economic University
celt@inbox.ru
Bolshaya Sadovaya St., 69, 344002 Rostov-on-Don, Russian Federation

Abstract. Over the past few decades, there has been a tendency to minimize the participation of the human factor in various production and other processes. This process is implemented through the mass introduction of automated systems. Man-machine complexes are currently the most common and productive model of activity.

At the current stage of technology development, the process of human activity automation is only an intermediate link on the way to excluding human intervention. This direction is the most relevant for systems that have a potential and real threat to human health and life (for example, manufacturing plants) or systems that are threatened by a person (for example, transport systems). The second group includes the sphere of information security. There is a need to move to the next level of excluding the human factor – introducing adaptive systems that will transfer the process of information protection in a completely different plane.

The organization of adaptive information security systems is based on applying existing methods of adaptation from other areas of scientific knowledge in relation to information security issues. Features of such application of the generalized principles of adaptation reflect the specifics of the subject area without violating generally accepted norms.

This article discusses the general principles of adaptive systems. It investigates the existing approaches to the organization of adaptive information security systems as well.

Key words: information security, adaptive information security systems, biosystem adaptation, typical model of the adaptive information protection system, organization of information security systems.