DOI: https://doi.org/10.15688/NBIT.jvolsu.2019.4.2

УДК 004.4
ББК 30.1

ПОСТРОЕНИЕ АДАПТИВНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Марина Ивановна Ожиганова

Заведующая кафедрой «Информационная безопасность»,
Севастопольский государственный университет
m.i.ozhiganova@sevsu.ru
ул. Университетская, 33, 299001 г. Севастополь, Российская Федерация

Анастасия Олеговна Калита

Доцент кафедры «Информационная безопасность»,
Севастопольский государственный университет
aokalita@sevsu.ru
ул. Университетская, 33, 299001 г. Севастополь, Российская Федерация

Евгений Николаевич Тищенко

Заведующий кафедрой «Информационная безопасность»,
Ростовский государственный экономический университет (РИНХ)
celt@inbox.ru
ул. Большая Садовая, 69, 344002 г. Ростов-на-Дону, Российская Федерация

Аннотация. Рассмотрены основы организации адаптивных систем защиты информации, их области применения для защиты информации и методы построения моделей адаптивных систем защиты информации в контексте применения их для защиты от утечки по техническим каналам. Предложена обобщенная модель адаптивной системы защиты информации от утечки по техническим каналам.

Ключевые слова: адаптивные системы защиты информации, адаптивное управление, каналы утечки информации, информационная безопасность, автоматизированные системы.

Введение

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 (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 здоровью и жизни человека (например, заводы обрабатывающей промышленности) или системы, угрозой которым является человек (например, транспортные системы). Ко второй группе можно отнести сферу информационной безопасности.

Так, служба безопасности IBM Managed Security Services в отчете «IBM Security Services 2014 Cyber Security Intelligence Index» на основании статистики, собранной в 2013 году по инцидентам в компьютерных сетях около 1000 клиентов из 133 стран, показывает, что подавляющее число инцидентов начинается с человеческой ошибки [10]. И это только один из многочисленных примеров.

Следовательно, существует необходимость в переходе на следующий уровень исключения человеческого фактора – внедрение адаптивных систем, которые позволят перенести процесс защиты информации в совершенно иную плоскость. Данный принцип активно внедряется в системы обеспечения компьютерной безопасности. Так, Ф.Г. Нестерук и Г.Ф. Нестерук на протяжении многих лет проводят исследования и разработки в области адаптивной защиты компьютерных систем и сетей (совместно с Котенко И.В., А.В. Шоровым и другими авторами). Также вопросу построения обобщенных моделей функционирования систем и средств защиты информации посвящены работы В.Г. Жукова, М.Н. Жуковой, И.А. Коромысловой, Е.С. Абрамова, А.В. Суханова, В.И. Крылова, И.М. Левкина, А.А. Володиной.

Целью данной работы является анализ существующих исследований в области построения адаптивных систем защиты информации и актуальных разработок в данной области.

Основы организации адаптивных систем защиты информации

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 [8, с. 17];

– структурная адаптация: адаптация структуры модели, допускающая сохранение значений параметров системы [8, с. 18].

Помимо классификации, необходимо рассмотреть обобщенный алгоритм построения моделей адаптируемых 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 подымается не впервые. Существуют как типовые модели адаптивной системы защиты информации (СЗИ), так и прикладные модели, учитывающие особенности конкретных областей защиты информации.

При исследовании существующих моделей адаптивных СЗИ, следует начать с рассмотрения типовой адаптивной СЗИ (см. рис. 1) [3].

Как видно из типовой модели, приведенной 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.

Проблематика применения принципов структурной адаптации в системах защиты информации заключается в нецелесообразности системных изменений в случае применения ее к системе технической защиты информации. Данный подход актуален для слу-

чаев, когда структура угроз информационной безопасности может изменяться с течением времени. Однако, природа технических каналов утечки информации остается неизменной, поскольку основывается на физических законах распространения информационных сигналах.

На основании модели структурной адаптации приемущественно разрабатываются самообучающиеся модели. Тем не менее, принцип самообучения используется также в системах с параметрической адаптацией.

Обобщенная архитектура адаптивного самообучающегося средства защиты информации приведена на рисунке 2 [4].

Обобщенно данную архитектуру можно описать как взаимосвязь трех структурных блоков:

– блок информационной системы;

– блок анализа состояния информационной системы;

– блок управления состоянием информационной системой.

Где блок анализа состояния ИС состоит из средств фиксации состояния ИС, базы данных состояний системы для дальнейшего накопления статистики и непосредственно средство анализа данных и генерации сценариев реагирования. Такая архитектура применима как к средствам ЗИ, как элементам СЗИ, так и к системе в целом.

В обобщенном виде данная структура процесса обучения адаптивной СЗИ является широко применимой

Основная область применения адаптивных СЗИ на текущий момент времени – обеспечение информационной безопасности в информационных технологиях (ИТ).

Такие системы строятся на биосистемных аналогиях между эволюцией биосистем и систем информационных технологий. В качестве перспективного метода разработки систем информационной безопасности (ИБ) рассматривается использование подобия механизмов защиты информационных процессов биосистем в искусственных системах [5].

Биосистемная аналогия систем информационных технологий представлена на рисунке 3 [5].

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

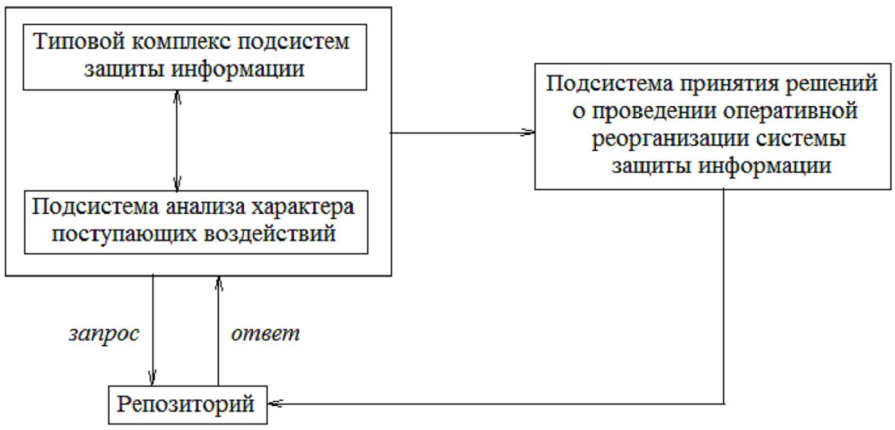

Рис. 1. Типовая адаптивная СЗИ

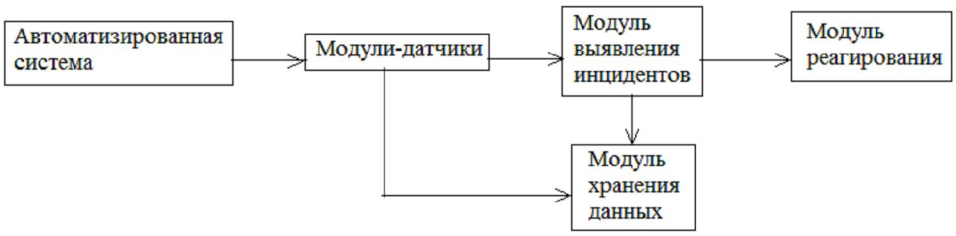

Рис. 2. Архитектура адаптивного самообучающегося средства ЗИ

– нижний уровень – механизмы иммунной системы;

– верхний уровень – механизмы адаптивной памяти и накопления жизненного опыта [11].

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

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

– описание и построение модели поведения биосистемы;

– непосредственное использование биологических аналогий в компьютерных системах [6].

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

Методы построения моделей систем защиты информации с адаптивным управлением

Методы построения моделей адаптивных систем строятся на аналогиях с существующими механизмами адаптации. Основным источником шаблонов таких механизмов является живя природа. Такие принципы называются биосисемными аналогиями. Они подразумевают перенос алгоритмов адаптации из биологических систем в технические системы. Так, как было указанно ранее следует рассматривать два основных подхода: применение принципов иммунных реакций и использование механизмов накопления знаний и жизненного опыта.

В биосистемах функции иммунной реакции реализуются в комплексе комбинации оперативной реакции на угрозы и дестабилизирующие воздействия и долговременных процессов [9].

Алгоритмы искусственных иммунных систем используются для решения следующих задач:

– обнаружение вторжений в компьютерных системах;

– распознавание новых видов вирусов и вредоносного программного обеспечения;

– управление инцидентами информационной безопасности;

– индексирование содержимого корпоративных сетей;

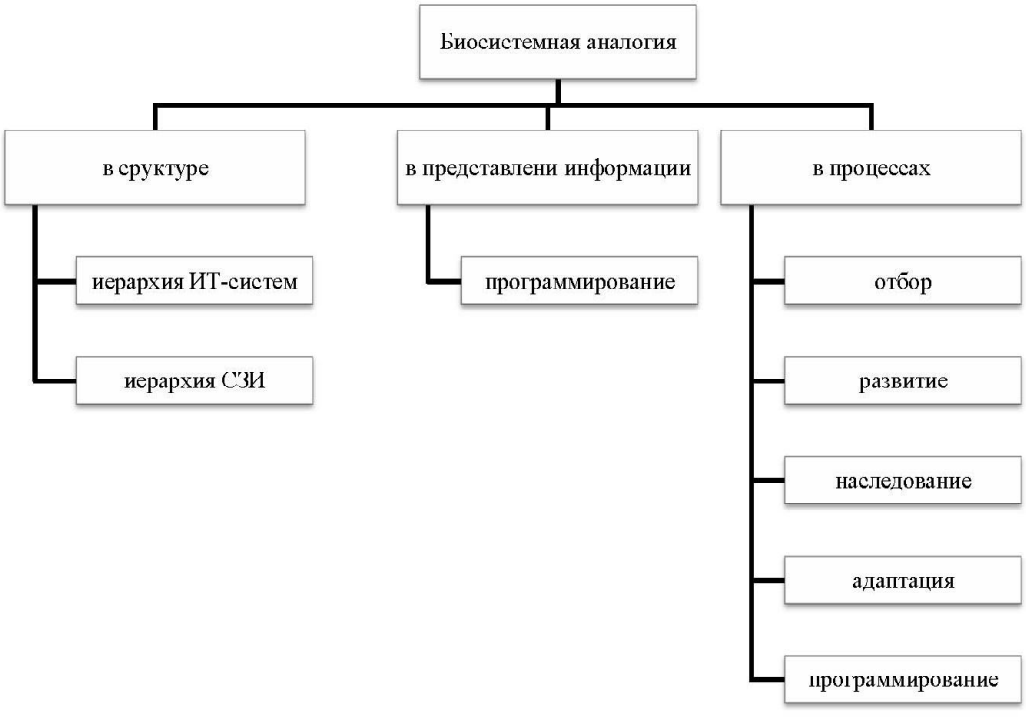

Рис. 3. Биосистемная аналогия ИТ-систем

– обнаружение неавторизированных устройств и пользователей и т. д. [2, с. 113].

Каждая из перечисленных задач строится, в первую очередь, на обнаружении аномалий. Алгоритм обнаружения аномалий:

1. Сбор данных для характеристики нормального состояния системы.

2. Формирование диапазона изменчивости (минимальные и максимальные значения области допустимых значений).

3. Кодирование критериев в форму, распознаваемую системой.

4. Определение объема паттерна данных.

5. Выделение паттернов данных для формирования массива сравнения.

6. Формирование детекторов для определения объектов, не входящих в область допустимых значений.

7. Мониторинг процессов на соответствие и реагирование на инциденты [1].

Процесс генерации детекторов (п. 1–6) в схематическом виде представлен на рисунке 4 [4].

Следующим этапом развития процесса генерации детекторов является применение модифицированного алгоритма клональной селекции (алгоритм представлен на рисунке 5) [7]. Данный алгоритм может использоваться как подсистема адаптивной системы защиты информации, так и в качестве отдель-

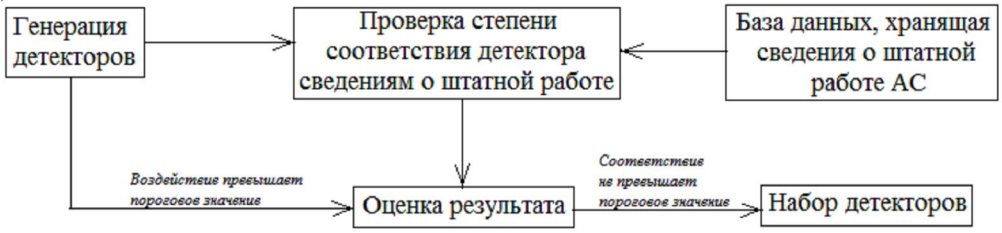

Рис. 4. Схема процесса генерации детекторов

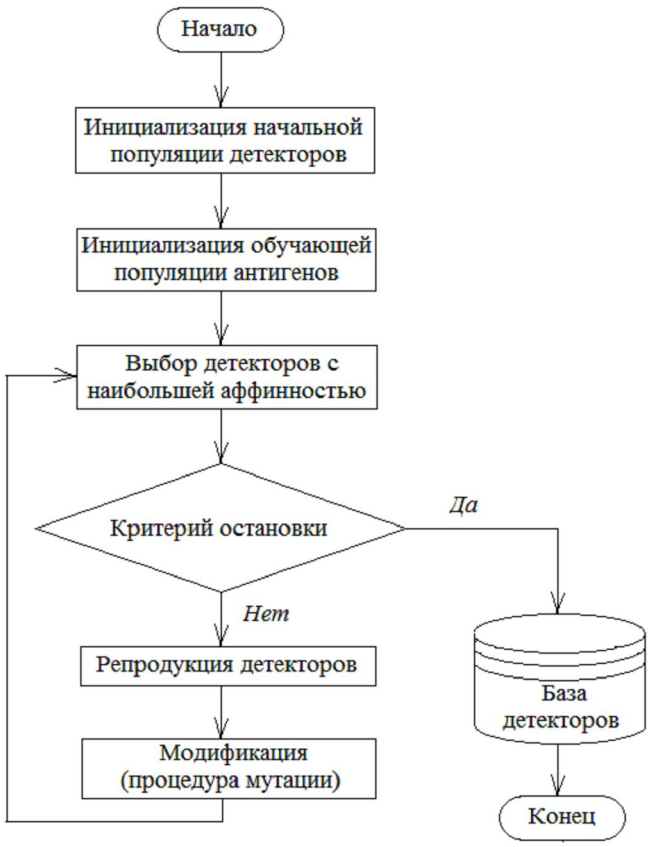

Рис. 5. Модифицированный алгоритм клональной селекции

ной системы, формирующей массив данных для использования его множеством адаптивных систем.

После выработки детекторов наступает этап мониторинга и реагирования (непосредственное функционирование адаптивной СЗИ). В системе, представленной на рисунке 6, выработка ответа системы на воздействие осуществляется посредством функции принятия решений, которая осуществляет следующие действия:

1) детектирование;

2) идентификация дестабилизирующих факторов;

3) подбор катастрофоустойчивого решения и анализ эффективности его применения;

4) реагирование [7].

На основании описанных методов построения систем адаптивной защиты информации строятся исключительномодели обнаружения аномалий и предотвращения инцидентов информационной безопасности,поскольку системы иммунной реакции направлены на идентификацию и противодействие недекларированым воздействиям на систему, что не соотносится с принципами защиты от утечки по техническим каналам.

Системы же накопления знаний и жизненного опыта могут быть использованы для обеспечения защиты информации как на уровне обнаружения и предотвращения злоумышленных активных) действий, так и на уровне поддержки состояния корректного функционирования системы путем мониторинга показателей работоспособности СЗИ.Следовательно, их можно рассматривать как потенциально применимый для рассматриваемой предметной области, но в виде общего подхода.

Формирование обобщенной модели защиты информации от утечки по техническим каналам с применением методов адаптивного управления

Система защиты информации от утечки по техническим каналам строится на комбинации активных и пассивных средств защиты информации. Пассивные средства направлены на устранение излишнего излучения полезного сигнала за пределы контролируемой зоны путем создания «барьеров» для прохождения сигналов: звукоизоляция, экранирование и др. Активные средства защиты информации направлены на зашумление среди распространения полезного сигнала.

Адаптивная система защиты информации от утечки по техническим каналам должна основываться на построении системы управления уровнем защищенности информации посредством применения активных средств защиты информации.

Структура разрабатываемой системы адаптивной ЗИ, в первую очередь должна удовлетворять общим требованиям по технической защите информации. Так, при рассмотрении данной области защиты информации, из трилогии «конфиденциальность-целостность-доступность», следует акцентировать внимание на обеспечении конфиденциальности, поскольку техническая защита информации подразумевает предотвращение утечек информации с ограниченным доступом.

Для начала следует рассмотреть структуру технического канала утечки информации:

1) источник полезного (информативного) сигнала;

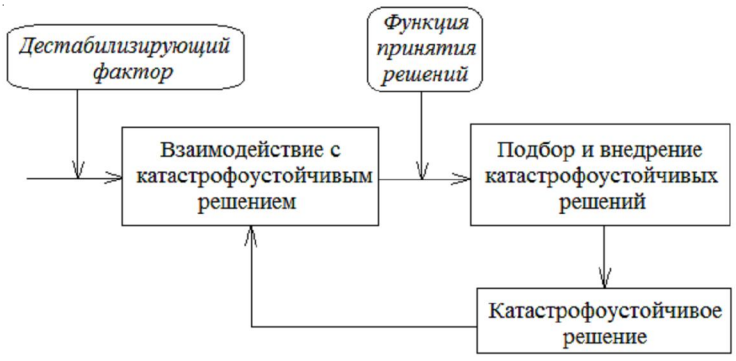

Рис. 6. Система реагирования адаптивной СЗИ на дестабилизирующие воздействия

2) среда распространения сигнала (физическое поле);

3) средство фиксации информативного сигнала (негласного съема информации).

Технический канал утечки информации с применением средств защиты информации функционирует по схеме, представленной на рисунке 7.

Система адаптивной защиты информации должна включать компоненты с функциями идентификации уровня защищенности, адаптации параметров элементов защиты и реализации алгоритмов адаптации (рис. 8).

Как видно на рисунке, система представляет собой циклическую модель, поскольку она должна обеспечивать обратную связь

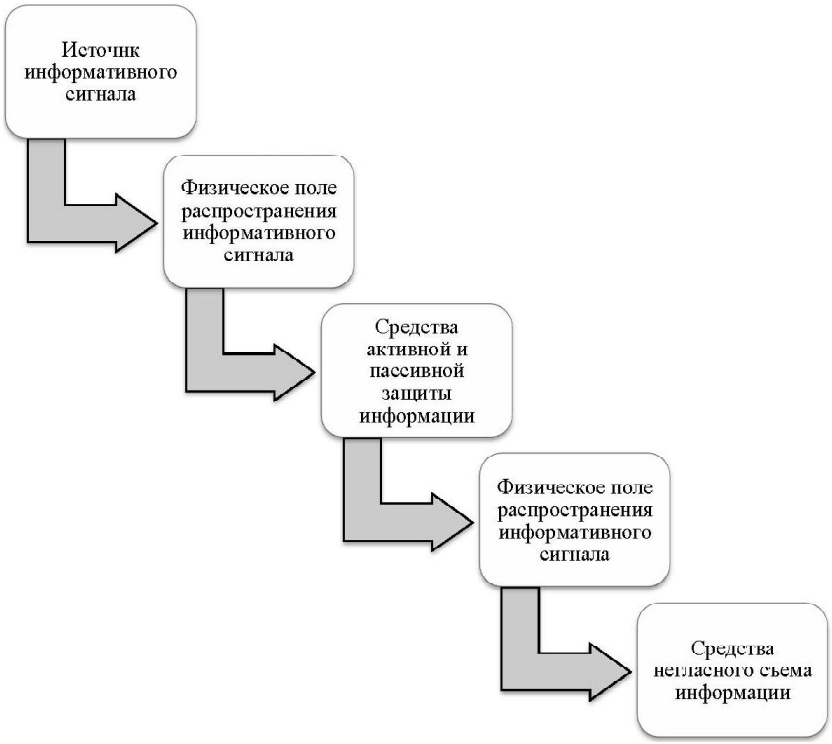

Рис. 7. Структура технического канала утечки информации

Рис. 8. Схема функционирования адаптивной системы защиты информации от утечки по техническим каналам

между модулем адаптации и защищаемой системой для корректного функционирования механизма управления СЗИ.

Проблема, на решение которой направлена разрабатываемая модель, это обеспечение необходимого и достаточного уровня зашумляющего сигнала в соответствии с уровнем информативного сигнала. На рисунке 9 представлена визуализация такого процесса: при установлении заданного начального уровня (прямой график) шумового сигнала, он может не соответствовать уровню «полезного» сигнала (волнистый график), где возможны случаи как излишнего зашумления, так и недостаточного.

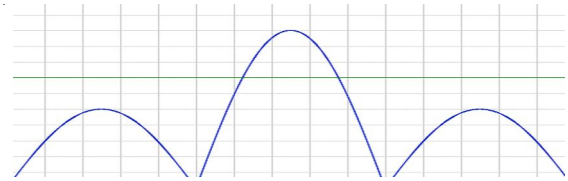

Рис. 9. Визуализация соотношения уровня информативного сигнала (волнистый график) и уровня шумового сигнала (прямой график)

Так, разрабатываемая модель должна решать следующие задачи:

1) обеспечение защиты информации в режиме реального времени;

2) поддержание уровня маскирующего сигнала, коррелирующего с информативным сигналом;

3) генерация маскирующего шумового сигнала.

Заключение

Рассмотренные и выделенные подходы к организации адаптивных систем защиты информации являются достаточно обобщенными для их широкого применения. Однако, в рамках данных подходов существует большое число методов построения моделей СЗИ, которые необходимо исследовать для определения степени их применимости к области технической защиты информации.

Проведен анализ существующих методов построения моделей адаптивных систем защиты информации. На основе проведенного исследования научных работ выведены основные закономерности функционирования адаптивных СЗИ в ИТ-системах, их преимущества и недостатки. Так, рассмотрев модели, основанные на функциях иммунных систем, можно сделать вывод о применимости таких моделей к блокированию технических каналов утечки информации: такие системы несовместимы с процессом обеспечения технической защиты информации.

Также сформированы требования к разрабатываемой системе защиты информации на основе принципов построения адаптивной системы и предложена обобщенная модель системы адаптивной защиты информации от утечки по техническим каналам.

СПИСОК ЛИТЕРАТУРЫ

1. Абрамов, Е. С. Построение адаптивной системы информационной безопасности / Е. С. Абрамов // Известия ЮФУ. Технические науки. – 2009. – № 11. – С. 99–109.

2. Васильев, В. И. Интеллектуальные системы защиты информации : учеб. пособие / В. И. Васильев. – М. : Машиностроение, 2013. – 172 с.

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

4. 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). – С. 18–23.

5. К разработке модели адаптивной защиты информации / Г. Ф. Нестерук [и др.]. – Электрон. текстовые дан. – Режим доступа: http://www.bnti.ru/showart.asp?aid=670&lvl=04. – Загл. с экрана.

6. Котенко, И. В. Анализ биоинспирированных подходов для защиты компьютерных систем и сетей / И. В. Котенко, А. В. Шоров, Ф. Г. Нестерук. – Электрон. текстовые дан. – Режим доступа: http://www.mathnet.ru/links/6dd22b2a6595ceea5c900fbc547fd9f5/trspy450.pdf. – Загл. с экрана.

7. Попелло, М. В. О применении искусственных иммунных систем в системах превентивной защиты информации / М. В. Попелло, М. В. Субботин, Н. А. Тишина. – Электрон. текстовые дан. – Режим доступа: https://interactive-plus.ru/e-articles/176/Action176-12348.pdf. – Загл. с экрана.

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

9. Суханов, А. В. Адаптивная защита информационных систем / А. В. Суханов, А. И. Крылов // Приборостроение. – 2008. – № 12. – С. 17–22.

10. Человеческий фактор – причина 95 % инцидентов ИБ. – Электрон. текстовые дан. – Режим доступа: https://xakep.ru/2014/06/19/62661. – Загл. с экрана.

11. Nesteruk, Ph. Information Safety in Electronic Business: Adaptive Model of Systems Safety of Information Technologies / Ph. Nesteruk, A. Kharchenko, G. Nesteruk // Proc. of Int. Conf. "Information technology in business" (St. Petersburg, October 8–10, 2003). – Saint Petersburg : [s. n.], 2003. – P. 124–128.

REFERENCES

1. Abramov E.S. Postroenie adaptivnoy sistemy informatsionnoy bezopasnosti [The Construction of Adaptive Systems of Information Security]. *Izvestiya YUFU. Tekhnicheskie nauki*, 2009, no. 11, pp. 99-109.

2. Vasilyev V.I. *Intellektualnye sistemy zashchity informatsii : ucheb. posobie* [Intelligent Information Security Systems]. Moscow, Mashinostroenie Publ., 2013. 172 p.

3. Volodina A.A., Levkin I.M. *Tipovaya struktura i sostav adaptivnoy sistemy zashchity informatsii bolshoy informatsionnoy sistemy* [Typical Structure and Composition of Adaptive Information Protection System of a Large Information System]. URL: http://ubs.mtas.ru/bitrix/components/bitrix/forum.interface/show_file.php?fid=16693.

4. Zhukov V.G., Zhukova M.N., Koromyslov N.A. Primenenie nechetkikh iskusstvennykh immunnykh sistem v zadache postroeniya adaptivnykh samoobuchayu-shchikhsya sredstv zashchity informatsii [Application of Fuzzy Artificial Immune Systems in the Task of Building Adaptive Self-Learning Information Protection Tools]. *Sibirskiy zhurnal nauki i tekhnologiy*, 2012, no. 1 (41), pp. 18-23.

5. Nesteruk G.F., Osoveckij L.G., Nesteruk F.G., Fahrutdinov R.Sh. *K razrabotke modeli adaptivnoy zashchity informatsii* [To Develop a Model of Adaptive Information Protection]. URL: http://www.bnti.ru/showart.asp?aid=670&lvl=04.

6. 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]. URL: http://www.mathnet.ru/links/6dd22b2a6595ceea5c900fbc547fd9f5/trspy450.pdf.

7. Popello M.V. Subbotin M.V., Tishina N.A. *O primenenii iskusstvennykh immunnykh sistem v sistemakh preventivnoy zashchity informatsii* [On the Use of Artificial Immune Systems in Preventive Information Protection Systems]. URL: https://interactive-plus.ru/e-articles/176/Action176-12348.pdf.

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

9. Suhanov A.V., Krylov A.I. Adaptivnaya zashchita informatsionnykh sistem [Adaptive Protection of Information Systems]. *Priborostroenie*, 2008, no. 12, pp. 17-22.

10. *Chelovecheskiy faktor – prichina 95 % intsidentov IB* [The Human Factor is the Cause of 95% of IS Incidents]. URL: https://xakep.ru/2014/06/19/62661.

11. Nesteruk Ph., Kharchenko A., Nesteruk G. Information Safety in Electronic Business: Adaptive Model of Systems Safety of Information Technologies. *Proc. of Int. Conf. "Information technology in business" (St. Petersburg, October 8–10, 2003)*. Saint Petersburg, 2003, pp. 124-128.

BUILDING ADAPTIVE INFORMATION SECURITY SYSTEMS

Marina I. Ozhiganova

Head of the Department "Information Security",
Sevastopol State University
m.i.ozhiganova@sevsu.ru
Universitetskaya St., 33, 299001 Sevastopol, Russian Federation

Anastasia O. Kalita

Associate Professor, Department "Information Security",
Sevastopol State University
aokalita@sevsu.ru
Universitetskaya St., 33, 299001 Sevastopol, Russian Federation

Yevgeny N. Tishchenko

Head of the Department "Information Security",
Rostov State University of Economics (RINH)
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 (as). Human-machine complexes are currently the most common and productive model of activity. At the current stage of technology development, the process of automating human activity is only an intermediate link on the way to eliminating human intervention. This area is most relevant for systems that pose a potential and real threat to human health and life (for example, manufacturing plants) or systems that are threatened by humans (for example, transport systems). The second group includes the sphere of information security. The paper considers the basics of the organization of adaptive information protection systems, their application areas for information protection and methods of building models of adaptive information protection systems in the context of their application for protection against leakage through technical channels. The authors propose a generalized model of the adaptive information protection system against leakage through technical channels.

Key words: adaptive information security systems, adaptive management, information leakage channels, information security, automated systems.