НАПРАВЛЕНИЯ РАЗВИТИЯ И ЗАДАЧИ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ АДАПТИВНЫХ СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

М.М. Добрышин*, к.т.н., Академия ФСО России, dobrithin@ya.ru.*

УДК 004.942

Аннотация. В статье проведен краткий анализ тенденций развития систем обеспечения информационной безопасности, определены общие недостатки применяемого математического аппарата и подходов, применяемых при синтезе адаптивных систем. На основании проведенного анализа сформулированы частные научные задачи, при решении которых на этапе проектирования адаптивных систем, возможно повысить их эффективность. На основании анализа отдельных законов информационной безопасности, сформулирован подход к определению финансовых затрат на синтез, эксплуатацию и модернизацию рассматриваемой системы.

Ключевые слова: теория информационной безопасности; система обеспечения информационной безопасности; адаптация.

DIRECTIONS OF DEVELOPMENT AND TASKS OF IMPROVING THE EFFICIENCY OF ADAPTIVE INFORMATION SECURITY SYSTEMS

M.M. Dobryshin, *Candidate of Technical Science, Academy of the FSO of Russia, employee.*

Annotation. The article provides a brief analysis of trends in the development of information security systems, identifies common shortcomings of the applied mathematical apparatus and approaches used in the synthesis of adaptive systems. On the basis of the analysis, private scientific tasks are formulated, in solving which, at the design stage of adaptive systems, it is possible to increase their efficiency. Based on the analysis of individual laws of information security, an approach to determining the financial costs of synthesis, operation and modernization of the system in question is formulated.

Keyword: information security theory; information security system; adaptation.

Введение

Развитие телекоммуникационной отрасли и проникновение ее во все сферы деятельности современного общества, способствует совершенствованию и появлению все новых видов и способов применения компьютерных атак (КА). Реагируя на инциденты информационной безопасности (ИБ), совершенствуется и система обеспечения информационной безопасности (СОИБ) корпоративных сетей связи (КСС). Однако данный процесс, с одной стороны, требует временных затрат на устранение выявленной уязвимости, а с другой стороны, вследствие инцидента ИБ, ущерб активам компании уже нанесен. В результате затраты на функционирование СОИБ можно отнести к убыткам. Расследования инцидентов ИБ ведущими организациями в данной сфере свидетельствуют, что значительная доля причин возникновения уязвимостей связана с человеческим фактором (за рамки исследования стоит отнести как инсайдеров, так и специалистов с низкой квалификацией). С целью устранения указанного фактора разрабатываются и эксплуатируются различные СОИБ, способные адаптироваться к новым видам КА,

в которую могут входить до 16 видов различных средств защиты от компьютерных атак (СЗ КА), соединенных между собой (рис. 1)[1]:

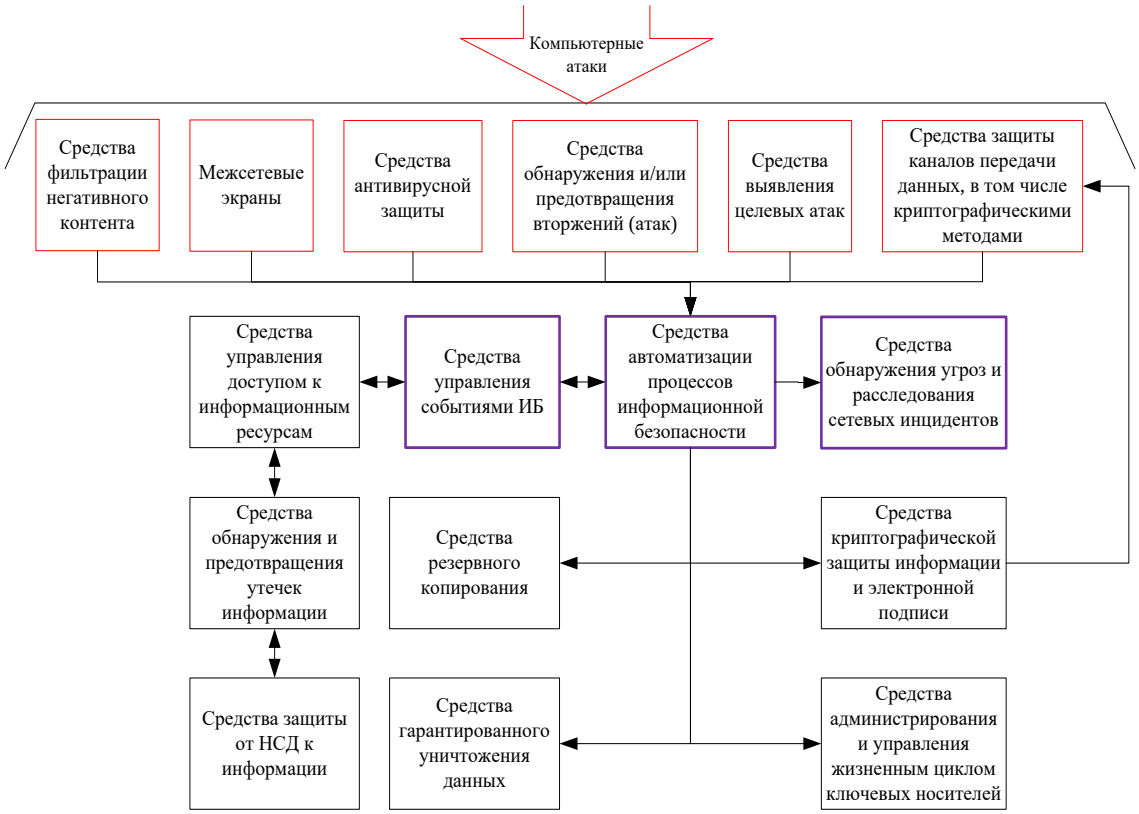

Рисунок 1

Тенденции развития систем обеспечения информационной безопасности

Одним из успешных проектов по защите от отдельных видов КА, являются продукты Лаборатории Касперского. Стоит отметить, что современные антивирусные средства совмещают традиционные-сигнатурные методы обнаружения вредоносного программного обеспечения (ВПО) и методы машинного обучения. Одной из основных причин высокой эффективности продуктов Лаборатории Касперского является то, что все программные средства, подключенные к интернету, сообщают об инцидентах ИБ, на которые в достаточно короткие сроки разрабатывают обновления, формируются новые правила и рассылаются всем программным средствам, тем самым, не давая возможности распространению выявленного ВПО по мировому информационному пространству и возникновению эпидемий. Рассматривая данный пример, можно говорить о созданной системе защиты от ВПО, причем способной адаптироваться к новым угрозам [1].

Вместе с тем, несмотря на то, что применение ВПО, занимает достаточно большую долю среди событий ИБ (до 40%, в зависимости от отрасли), они не наносят значительного ущерба (до 10 % от всего ущерба, в зависимости от отрасли) [2]. Причем статистические данные свидетельствуют о том, что для повышения эффективности своих действий злоумышленники все чаще применяют в

[1] Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 22 сентября 2020 г. № 486. Об утверждении классификатора программ для электронных вычислительных машин и баз данных / Зарегистрировано в Минюсте России 29 октября 2020 г. № 60646.

отношении КСС APT-атаки (таргетированных, групповых разнородных атак) [3]. Особенностью таких КА является то, что злоумышленник применяет (последовательно или параллельно) несколько видов КА, что вносит значительную неопределенность в процесс принятия решения и как следствие неправильные или несвоевременные действия, приводящие к успешности КА. Логическим этапом развития теории ИБ стало применение элементов искусственного интеллекта в СЗ КА и их объединение в единую систему – систему обеспечения информационной безопасности [4].

Применение элементов искусственного интеллекта (генетические алгоритмы, нейросети, элементы нечеткой логики) позволяет за счет выявления неявных связей и обработки большого объема данных повысить эффективность СЗ КА.

Генетические алгоритмы в качестве основных механизмов формирования правил применяют функцию приспособляемости, которая в зависимости от выявленной КА на основании мутации и скрещивания генов позволяет определить схему или стратегию действий на несколько шагов вперед (при условии, что воздействия не претерпят существенного изменения), при достаточно небольших вычислительных затратах (выбор варианта осуществляется не путем полного перебора всех вариантов, а за счет указанных правил мутации и скрещивания). Также возможность формирования стратегии применения нескольких элементов во времени позволяет повысить экономичность схемы, за счет подключения элементов по необходимости) [5, 6].

Нейросети. Принцип работы адаптивных СОИБ на основе нейросетей заключается в том, что за каждое совершенное действие получают «подкрепление», т.е. заданное число, которое может быть положительным (награда – если элемент успешно справился с адаптацией) и отрицательным числом (наказание – если действия элемента не принесли требуемого результата). Развитием метода обучения с подкреплением, являются решения, направленные на формирование правил и градаций начисления наград (наказаний), награждение не только элемента, действия которого достигли требуемого эффекта и его предшественников, а также формирование из элементов устойчивых цепочек и их награждение [6, 7].

Элементы нечеткой логики. Принятие решения в условиях неопределенности об адаптации производится на основании поэтапного приближения. Формирование нечетких правил принятия решения позволяет в значительной мере повысить достоверность классификации, выявленной КА, что позволяет более обоснованно применять имеющиеся СЗ КА. Принцип нечеткой логики позволяет применять различный математический аппарат для описания динамики функционирования СОИБ [8, 9].

Наряду с достоинствами применения элементов искусственного интеллекта указанными ранее, существуют и определенные недостатки [10]:

- учитывая, что все перечисленные математические инструменты основаны на эвристических правилах – для адекватной адаптации СОИБ необходимы статистические данные о произошедших событиях, в том числе на других элементах КСС или большое количество инцидентов ИБ на защищаемом элементе;
- обработка большого объема данных в реальном времени требует значительных вычислительных ресурсов;
- практический опыт показывает, что рассматриваемые средства достаточно хорошо справляются только с одним видом деятельности, вследствие чего схемы значительно усложняются при попытках решать несколько

независимых задач и как следствие возникают ошибки первого и второго рода при обработке информации между уровнями.

Однако, несмотря на указанные недостатки, практический опыт показывает (пример Лаборатории Касперского), что средства на основе искусственного интеллекта обеспечивают более высокую защищенность КСС от КА.

С ростом количества новых видов КА и увеличением интенсивности их появления возникла необходимость разрабатывать СОИБ способных самостоятельно реагировать на новые виды КА, т.е. адаптироваться. Под адаптивной СОИБ следует понимать систему, способную при выявлении событий или инцидентов ИБ изменяться, для обеспечения требуемого уровня защищенности КСС.

Основные задачи, решаемые системой с адаптацией, показаны на рис. 2.

Систему можно считать адаптивной, если она обладает следующими признаками [10-12]:

- уровень адаптации (структурная, алгоритмическая, параметрическая);
- механизм адаптации (с эталонной моделью, аналитически-настраиваемые, экстремальные, эвристические);
- способ адаптации (дискретная, непрерывная).

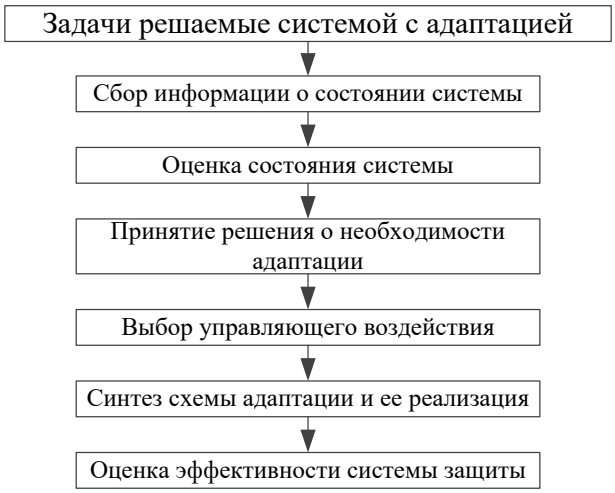

Рисунок 2

Адаптация СОИБ осуществляется за счет изменения [10-12]:

- структуры – изменение связей между СЗ КА или активации неиспользуемых ранее СЗ КА;
- алгоритмов работы – изменение, введение или отключение отдельных режимов и правил;
- параметров СЗ КА – увеличение полосы пропускания каналов связи, выделение дополнительных вычислительных мощностей для указанных процессов или элементов.

Вопрос выбора механизма адаптации рассматривались при анализе элементов искусственного интеллекта, более подробно анализ механизмов адаптации и один из возможных вариантов построения иерархического механизма адаптации рассмотрены в работе [10].

Способ адаптации в большинстве случаев определяется двумя основными факторами – динамикой изменения дестабилизирующих факторов и выделяемыми вычислительными ресурсами. Дискретная адаптация – оценка состояния и

необходимое изменение системы через заданные промежутки времени. Непрерывная адаптация – непрерывная оценка состояния системы и необходимое изменение системы. С диалектической точки зрения любой процесс дискретен и отличается друг от друга, только частотой дискретизации.

Для повышения адекватной адаптации СОИБ целесообразно обрабатывать статистические данные, поступаемые не только от СЗ КА, входящих в состав СОИБ, но и от средств оценки качества информационных потоков, предоставляемых услуг связи и режимов работы инфотелекоммуникационного оборудования КСС. Обработка данных о состоянии КСС позволяет сократить признаковое пространство (условия применимости КА) [13] и снизить время на обучение применяемого математического аппарата.

Задачи повышения эффективности адаптивных СОИБ

Анализ известных работ в предметной области [11-15], способов и механизмов применения КА [16], а также работ в области синтеза СОИБ [17-20] и квалиметрии [21-23], позволили сформулировать ряд недостатков, существующих адаптивных СОИБ, устранение которых будет способствовать повышению их эффективности:

- существующие СОИБ рассматриваются как совокупность СЗ КА, функционирующих как самостоятельные средства (однако СОИБ является подсистемой корпоративной сети связи). Обеспечение защиты корпоративной сети связи (КСС) рассматривается как защита узлов (элементов), входящих в КСС (обмен данными об инцидентах и событиях ИБ между узлами КСС не осуществляется или осуществляется со значительной задержкой);
- целеполагание функционирования СЗ КА основано на обеспечение ИБ защищаемой информации, средств обработки хранения и передачи информации и сетевой безопасности без учета влияния на процесс организации связи, вследствие чего СЗ КА затрудняют или блокируют функционирование КСС (как следствие СЗ КА отключают);
- принятые подходы оценки качества СОИБ (обеспечение целостности, доступности и конфиденциальности защищаемой информации) не отражают протекающие в самой системе процессов и не позволяют судить о ее эффективности, как в статичном, так и динамическом состоянии;
- недостаточно проработанные аксиоматический аппарат и таксономические категории, и схемы квалиметрии в области оценки качества СОИБ (существующие подходы не в полной мере позволяют определить назначение, цель, задачи, функции, свойства, параметр, показатель и др. в области квалиметрии ИБ);
- недостаточно проработанный методический аппарат в области оценки эффективности функционирования СОИБ (решаемая задача относится к области многокритериальных задач, причем эффективность СОИБ со временем изменяется, однако существующие подходы позволяют дать только точечные оценки).

Таким образом, адаптивная СОИБ – это сложная техническая система, являющаяся подсистемой КСС, при синтезе которой необходимо решить следующие задачи:

- сформулировать единое целеполагание функционирования СОИБ КСС и входящих в ее состав СЗ КА (СОИБ предназначена для обеспечения функционирования КСС), определить частные задачи и функции по обеспечению защищенности КСС от КА;

- определить системные свойства, описывающие функционирование СОИБ КСС, как сложной технической системы;
- задать квалиметрическую шкалу и систему оценки качества СОИБ КСС;
- определить структуру, включающую группу СЗ КА, информационные связи как между отдельными СЗ КА, так и между СЗ КА, расположенными на различных узлах КСС, а также связи с другими подсистемами КСС, осуществляющими обмен данными о событиях и инцидентах ИБ в реальном времени (псевдореальном – время необходимое на обработку и передачу данных);
- разработать алгоритмы и правила, позволяющие управлять адаптацией СОИБ КСС в зависимости от видов, выявленных КА;
- сформулировать порядок оценки эффективности функционирования адаптивной СОИБ.

Подход к определению финансовых затрат на синтез, эксплуатацию и модернизацию СОИБ

Под качеством понимается сложное диалектическое понятие, отражающее совокупность эмерджентных свойств СОИБ, а под эффективностью понимается мера качества. Причем вопросы оценки качества с идеологической точки зрения значительно шире вопросов оценки эффективности СОИБ. Так оценка качества СОИБ проводится на всех этапах жизненного цикла СОИБ, а вопросы оценки эффективности только на этапе функционирования этой системы. Однако именно результаты оценки эффективности являются основанием для модернизации и дальнейшей оценки качества СОИБ.

Также в настоящее время не в полной мере определены критерии, позволяющие обоснованно определить объем финансирования проектирования, эксплуатации и модернизации СОИБ КСС. Ведь как говорилось ранее, если ущерб от КА был нанесен, то затраты на разработку и эксплуатацию СОИБ являются убытками КСС. Принятый подход, основанный на выборе СОИБ, обладающей минимальной стоимостью и не в полной мере, отражает процесс обеспечения защищенности КСС, т.к. не учитывает ряд базовых законов ИБ [24]:

Закон Склярова. Если стоимость взлома объекта *А* больше выгоды от взлома этого объекта, то объект не будет взломан.

Основываясь на принципе рациональности, данный закон можно интерпретировать как: стоимость обеспечения ИБ не должна превышать стоимости защищаемой информации.

Таким образом, СОИБ должна создать такие условия, чтобы злоумышленнику было экономически невыгодно атаковать КСС, причем затраты на эксплуатацию СОИБ не должны превышать стоимость защищаемой информации.

Закон Батенева. Если стоимость взлома объекта *А* больше стоимости взлома объекта *Б*, то объект *А* не будет взломан до тех пор, пока не будет взломан объект *Б*.

В качестве примера следует рассмотреть ситуацию, когда главный узел КСС защищается большим количеством СЗ КА нежели региональные узлы КСС. Как следствие злоумышленник осуществит КА на менее защищенный узел. Однако, если пользователи регионального узла КСС имеют доступ к ресурсам главного узла КСС, то и у злоумышленника появляется потенциальный доступ. Исходя из этого, элементы СОИБ, расположенные на различных узлах КСС, должны выполнять идентичные функции и задачи (в рамках разветвленной КСС, с экономической точки зрения, эффективнее иметь унифицированные СЗ КА и алгоритмы взаимодействия между собой).

Заключение

Выделенные тенденции развития СОИБ, изменившиеся возможности злоумышленников, уточненные ранее тенденции развития теории информационной безопасности и квалиметрии, позволили сформулировать уточненные задачи синтеза. Сформулированные задачи рассматривают СОИБ, как сложную техническую систему, обладающую собственными свойствами, но функционирующую в составе и интересах корпоративной сети связи, а именно с целью обеспечения предоставления абонентам сети заданного количества услуг связи с требуемым качеством. Решение указанных задач позволит обоснованно выбрать адаптивную СОИБ с требуемым качеством, а сформулированный подход к определению объема финансирования проектирования, эксплуатации и модернизации СОИБ позволит обосновать расходы и избежать финансовых и иных убытков для компании.

Литература

1. Адаптивная архитектура: ключ к истинной кибербезопасности году [Электронный ресурс] // Kaspersky.ru [сайт]. – URL: http://kaspersky-ru.turbopages.org/kaspersky.ru/ s/blog/asa-key-to-true-cybersecurity/4599/ (дата обращения 15.08.2022).
2. Информационная безопасность в 2021 году [Электронный ресурс] // Positive Technologies [сайт]. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/ informa-cionnaya-bezopasnost-v-2021-samye-gromkie-vzlomy-i-utechki/ (дата обращения 15.08.2022).
3. APT-атаки на промышленные компании во второй половине 2021 года [Электронный ресурс] // Kaspersky.ru [сайт]. – URL: http//ics-cert-kaspercky.ru.turbopages.org/ics-cert.kaspersky.ru/s/publications/ reports /2022/02/28/apt-attacks-on-industrial-companies-in-h2-2021/ (дата обращения 15.08.2022).
4. Добрышин М.М., Шугуров Д.Е. Иерархическая многоуровневая модель таргетированных компьютерных атак в отношении корпоративных компьютерных сетей // Проблемы информационной безопасности. Компьютерные системы, 2020. – № 4. – С. 35-46.
5. Бобцов А.А., Никифоров В.О., Пыркин А.А., и др. Методы адаптивного и робастного управления нелинейными объектами в приборостроении: учебное пособие для высших учебных заведений. – СПб: НИУ ИТМО, 2013. – 277 с.
6. Рутковская Д., Пилиньский М., Рутковский Л. Нейронные сети, генетические алгоритмы и нечеткие системы; [пер. с польск. Д. Рудинского]. – М.: Горячая линия – Телеком. 2006. – 452 с.
7. Бураков М.В. Генетический алгоритм: теория и практика: учеб. пособие // М.В. Бураков. – СПб.: ГУАП, 2008. – 264 с.: ил.
8. Хижняков Ю. Н. Алгоритмы нечеткого, нейронного, нейронечеткого управления в системах реального времени. Пермь: ПНИПУ. 2013. – 160 с.
9. Усов А.Е., Варламов А.А., Бабкин О.В., и др. Применение парадигмы нечеткой кластеризации и бикластеризации при мониторинге инфраструктуры центров обработки данных // Современные инновации, 2018. – № 4 (32). – С. 15-21.
10. Добрышин М.М. Выбор структуры и механизмов адаптивного управления системы обеспечения информационной безопасности // Известия Тульского государственного университета. Технические науки, 2022. – № 2. – С. 214-222.
11. Лаврова Д.С., Зегжда Д.П., Александрова Е.Б., Калинин М.О. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам. Под ред. доктора технических наук, профессора Д.П.

Зегжды. – М.: Горячая линия – Телеком, 2019. – 640 с.: ил., ISBN 978-5-9912-0827-7.
12. Абрамов Е.С. Построение адаптивной системы информационной безопасности / Известия ЮФУ. Технические науки, 2009. – № 11. – С. 99-109.
13. Гречишников Е.В., Горелик С.П., Добрышин М.М. Способ обеспечения требуемой защищенности сети связи от внешних деструктивных воздействий // Телекоммуникации, 2015. – № 6. – С. 32-37.
14. Дроботун Е.Б. Теоретические основы построения систем защиты от компьютерных атак для автоматизированных систем управления / Монография. – СПб.: Наукоемкие технологии, 2017. – 120 с., ил.
15. Белов А.С., Добрышин М.М., Борзова Н.Ю. Формирование модели угроз информационной безопасности на среднесрочный период // Приборы и системы. Управление, контроль, диагностика, 2021. – № 7. – С. 41-48.
16. Добрышин М.М. Особенности применения информационно-технического оружия при ведении современных гибридных войн // I-methods, 2020. – Т. 12. – № 1. – С. 1-11.
17. Зегжда П.Д. Модель оптимального комплексирования мероприятий обеспечения информационной безопасности // Проблемы информационной безопасности. Компьютерные системы, 2020. – № 2. – С. 9-15.
18. Ожиганова М.И., Калита А.О., Тиченко Е.Н. Построение адаптивных систем защиты информации / Инновации в информатике // НБИ технологии, 2019. – Т. 13. – № 4. – С. 12-21.
19. Лясковский В. Л. Основы проектирования и эксплуатации автоматизированных систем управления военного назначения: учеб. пособие / под ред. доктора технических наук, профессора В.Л. Лясковского. – М.: Издательство МГТУ им. Н. Э. Баумана, 2016. – 188 с.: ил.
20. Щербаков А.Ю. Методы и модели проектирования средств обеспечения безопасности в распределенных компьютерных системах на основе создания изолированной программной среды: Дис. … докт. техн. наук: 05.13.12, 05.13.13 / А.Ю. Щербаков. – М.: Московский государственный институт электроники и математики, 1997. – 320 с.
21. Добрышин М.М. Подход к формированию обобщенного критерия оценки эффективности системы обеспечения информационной безопасности / Известия Тульского государственного университета. Технические науки, 2021. – № 9. – С. 113-121.
22. Андрианов Ю.М. Квалиметрия в приборостроении и машиностроении / Ю.М. Андрианов, А.И. Субетто. – Ленинград: Машиностроение. Ленингр. отделение, 1990. – 216 с.
23. Добрышин М.М. Тенденции развития теории информационной безопасности в условиях динамического изменения парадигмы применения информационно-технических воздействий // Экономика и качество систем связи, 2022. – № 1 (23). – С. 37-43.
24. Прохорова И.А. Теория систем и системный анализ: учебное пособие / И.А. Прохорова. – Челябинск: Издательский центр ЮУрГУ, 2013. – 49 с.