Scientific and Practical Cyber Security Journal (SPCSJ) 4(2): 63-71 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

АНАЛИЗ ИЗВЕСТНЫХ МЕТОДОВ И МЕТОДИК ДИАГНОСТИРОВАНИЕ КИБЕРНЕТИЧЕСКОЙ УСТОЙЧИВОСТИ ФУНКЦИОНИРОВАНИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЕ В КИБЕРНЕТИЧЕСКОМ ПРОСТРАНСТВЕ

Козубцова Леся Михайловна, Военный институт телекоммуникаций и информатизации, г. Киев, Украина
к.т.н., доцент Кит Григорий Васильевич, Ивано-Франковский филиал Открытого международного университета развития человека «Украина» г. Ивано-Франковск, Украина
к.т.н., профессор РАЕ Козубцов Игорь Николаевич, Научный центр связи и информатизации Военного института телекоммуникаций и информатизации, г. Киев, Украина

АННОТАЦИЯ. В статье проведен анализ известных методов и методик диагностирование кибернетической устойчивости функционирования информационной системы специального назначение в кибернетическом пространстве. Установлено, что на данное время существуют несколько однотипных решений, у которых отсутствуют объяснения каким образом осуществляется расчет некоторых составляющих параметров.

ЦЕЛЬЮ СТАТЬИ является апробация результатов анализа известных методов и методик диагностирование кибернетической устойчивости функционирования информационной системы специального назначение в кибернетическом пространстве.

Практическое значимость результата заключается в обосновании необходимости усовершенствования известных однотипных результатов до уровня их возможного практического применения.

КЛЮЧЕВЫЕ СЛОВА: *анализ, методика, диагностирование, кибернетическая устойчивость, защищенность, надежность, живучесть, информационная система специального назначения, деструктивное информационное влияние.*

ANALYSIS OF KNOWN METHODS AND TECHNIQUES DIAGNOSTICS OF CYBERNETIC STABILITY OF THE FUNCTIONING OF A SPECIAL PURPOSE INFORMATION SYSTEM IN CYBERNETIC SPACE

Lesya Kozubtsova, Military institute of telecommunications and informatization, Kiev, Ukraine
Ph.D., associate Professor Gregory Kit, Ivano-Frankivsk branch of the Open international University for human development "Ukraine" Ivano-Frankivsk, Ukraine
Ph.D., Professor RAE, Igor Kozubtsov Scientific center of communication and Informatization of the Military Institute of telecommunications and Informatization, Kiev, Ukraine

ABSTRACT. The article analyzes the known methods and techniques for diagnosing the cybernetic stability of the functioning of a special purpose information system in cybernetic space. It is established that at this time there are several solutions of the same type, which do not have explanations of how to calculate some of the component parameters.

The purpose of the article is to test the results of the analysis of known methods and techniques for diagnosing the cybernetic stability of the functioning of a special purpose information system in cybernetic space.

The practical significance of the result is to justify the need to improve the known results of the same type to the level of their possible practical application.

KEYWORDS: *analysis, methodology, diagnostics, cybernetic stability, security, reliability, survivability, special-purpose information system, destructive information influence.*

ВВЕДЕНИЕ

Современные информационные системы специальных пользователей используются для решения задач широкого спектра научных и производственных задач сбора, обработки, накопления и хранения информации с ограниченным доступом, управления критическими объектами в реальном масштабе времени. Решение данных задач является актуальным в повседневной деятельности специальных пользователей Украины и имеет важное значение для национальной безопасности Украины. Поскольку функционирование информационных системы специальных пользователей предусмотрено в киберпространстве, в котором существуют кибернетические уязвимости и угрозы [27; 28; 24], поэтому выдвигается высокий уровень требований к адекватности,

оптимальности, оперативности, устойчивости, непрерывности, скрытности [26; 1; 4; 23]. Из перечисленных требований, в диссертационном исследовании ограничимся рассмотрением «кибернетической устойчивости». Исходя из этого возникает научная задача разработки нового инструментария диагностирования кибернетической устойчивости функционирования ИС СН.

Под “кибернетической устойчивостью функционированием ИС СН» будем понимать состояние ее защищенности, которое обеспечивает устойчивое функционирование в условиях преднамеренных и случайных действий кибернетических деструктивных информационных воздействий (ДИВ).

Если не уделить должного внимания решению данного вопроса, то в контексте описания “Будущее безопасность среда 2030. Анализ стратегического предвидения” выполнено исследователи Военного института телекоммуникаций и информатизации в работах [10; 14; 13; 11] прогнозируют неминуемое наступление коллапса в различных сферах автоматизации и информатизации:

опасность искажения, подмена информации во всемирно известных электронных научно-технических библиотеках, энциклопедиях, наукометрических базах (библиотека им. В.И. Вернадского, Wikipedia, SciVerse Scopus, Web of Science (WoS), Google Scholar, и тому подобное [20; 12]);

вмешательство в работу оборудования – атаки на компьютеры или серверы, которые обеспечивают работу гражданских коммуникаций (нарушение системы водоснабжения, электроэнергии, транспорта и т. п) [5];

нарушение функционирования автоматизированных систем управления войсками (функциональный сбой и несанкционированное управления войсками и вооружением, как примера ход событий в научно-фантастическом фильме “Terminator”, где искусственный интеллект сети “SkyNet” получив доступ к управлению системой противоракетной обороны и ядерным вооружением Вооруженных сил США создал условия для уничтожения человечества. И хотя на первый взгляд это выглядит фантастически, но сегодняшние “кибервойны” и “киберпространство”, из научно-фантастического романа У. Гибсона “Нейромант” (1982), перекочевали в современную реальность [2].

За перечисленных последствий возможно нарушение функционирования информационно-телекоммуникационных систем, в результате так называемого коллапса. До появления коллапсов в информационно-телекоммуникационных системах в следствие кибернетических угроз, были известны лишь “экономический коллапс”, “экологический коллапс”, “финансовый коллапс”, “политический коллапс”, “социальный коллапс” и др.

Таким образом, если не уделить должного внимания решению данного вопроса, то прогнозируют неминуемое наступление коллапса в различных сферах автоматизации и информатизации, что приведет к нарушению национальной безопасности Украины.

ЦЕЛЬ СТАТЬИ

Апробировать результаты анализа известных методов и методик диагностирование кибернетической устойчивости (компонентов устойчивости) функционирования информационной системы специального назначение в кибернетическом пространстве

ОСНОВНОЙ РЕЗУЛЬТАТ

В соответствий с целью исследования проанализируем известны существующие подходы, методы и методики диагностирование информационной системы специального назначение в такой последовательности: «кибернетическая устойчивость», «кибернетическая надежность, «кибернетическая живучесть».

Проанализируем известные методы и методики диагностирование кибернетической устойчивости информационной системы специального назначения. Решение данной научной задачи начато с поиска в открытых источниках информации по ключевым словом «подходы методы и методики диагностирование кибернетической устойчивости функционирования информационной системы специального назначение».

На данный момент времени, благодаря Будапештской инициативе открытого доступа к научных публикаций (The Budapest Open Access Initiative) найдены следующие научные публикации [7; 21; 22; 3], в которых объектом исследования выступала киберустойчивость объектов критической информационной инфраструктуры (КИИ).

Проработав данные работы было установлено, что методика оценки киберустойчивости КИИ в общем виде состоит из следующих этапов:

1. Этап оценки киберустойчивости каждого объекта КИИ ($К_{\text{ОКИИ}}^{\text{уо}}$) отдельно (1).

$$К_{\text{ОКИИ}}^{\text{уо}} = К_{\text{ОКИИ}}^{\text{жив}} \times К_{\text{ОКИИ}}^{\text{пом}} \times К_{\text{ОКИИ}}^{\text{над}} \quad (1)$$

где $К_{\text{ОКИИ}}^{\text{жив}}$ – киберживучесть – живучесть объекта КИИ;

($К_{\text{ОКИИ}}^{\text{уо}}$) – киберзащищённость однозвенного объекта КИИ;

$К_{ОКИИ}^{над}$ – кибернадежность однозвенного объекта КИИ.

1.1 Оценка однозвенного объекта КИИ.

Оценка киберзащищённость – вероятность выхода из строя *i*-го технического средства обработки информации (ТСОИ) в условиях ДИВ.

Оценить коэффициент связанности *i*-го ТСОИ и его вклад в целевую функцию объекта КИИ.

Оценка киберживучести – предела состояний однозвенного объекта КИИ.

1.2. Оценка многозвенного объекта КИИ.

Оценка киберзащищённости – вероятность выхода из строя *j*-го однозвенного объекта КИИ в условиях воздействия ИИИ.

Оценить коэффициент связанности *j*-го однозвенного объекта КИИ и его вклад в целевую функцию многозвенного объекта КИИ.

Оценка киберживучести – предел состояний многозвенного объекта КИИ.

2. Этап оценки киберустойчивости взаимодействующих объектов КИИ (стволов объектов КИИ).

Оценка киберзащищённости – вероятность выхода из строя *n*-го многозвенного объекта КИИ в условиях воздействия ДИВ.

Оценить коэффициент связанности *n*-го многозвенного объекта КИИ и его вклад в целевую функцию многозвенного объекта КИИ.

Оценка киберживучести – предел состояний ствола КИИ.

3. Этап оценки киберустойчивости КИИ через сумму устойчивости ее элементов с учетом их коэффициента связности.

Оценка киберживучести КИИ в целом, соответственно до текущего состояния стволов КИИ и степенью важности, в данный момент времени, выполнения ими функций.

Для нашего исследования ценными являются работы [7; 21; 22], которые исследовали киберустойчивость КИИ. Однако авторы не раскрывают ни подходов, ни алгоритма оценки коэффициентов связности. В следствие этого невозможным практическое использование известной методики для специальных пользователей, что подтверждено попыткой экспериментальной проверки во время исследования на военных стратегических командно-штабных учениях с органами военного управления, войсками (силами) Вооруженных Сил Украины “Несокрушимая устойчивость – 2017” в период с 11.09.2017 по 26.09.1017 г. офицерами-исследователями Научного центра связи и информатизации Военного института телекоммуникаций и информатизации. Также известную методику нельзя сравнить с предложенной нами в диссертации, поскольку отсутствие сведений относительно коэффициентов связанности. Возможна через то, что разработкой методики занимались работники Краснодарского высшего военного училище им. генерала армии С.М. Штеменко, Российской Федерации (РФ) И.Д. Королев и Г.И. Захарченко и отдельные результаты могли составлять государственную тайну РФ, как следствие не подлежали к публикации в открытых источниках. Не исключение, детализация методики опубликована в научном сборнике с грифом «Секретно».

Таким образом, для обеспечение диагностирование кибернетической устойчивости ИС СН нуждается в совершенствование известны результаты [7; 21; 22].

На основании отсутствия сведений относительно нахождения коэффициентов связанности, необходимо усовершенствовать данную методику путем адаптации ее для обеспечения диагностирование кибернетической устойчивости ИС СН. Данное решение будет одной из научных задач нашего диссертационного исследования.

Проанализируем известные методы и методики диагностирование кибернетической надежности информационной системы специального назначения.

Надежность – это комплексная свойство, что включает в себя безотказность, ремонтопригодность и сохранность [19].

Безотказность – свойство системы или ее элементов непрерывно выполнять востребованную функцию в заданном интервале времени или некоторые наработки. Наработкой называют интервал времени, в течение которого изделие находится в состоянии функционирования.

Ремонтопригодность – способность системы при заданных условиях эксплуатации к поддержке или восстановлению состояния за счет технического обслуживание, в котором она может выполнять востребованную функцию.

Сохранностью называют способность системы выполнять востребованную функцию в течение и после хранения или транспортировки.

Комплексность понятие «надежность», с учетом выше сказанного, делает его фундаментальным, таким всесторонне охватывает техническую эксплуатацию систем и элементов. В свою очередь, надежность является

составной более широкого понятие эффективность, под которой понимают способность системы выполнять заданные функции с необходимой качеством.

Показателями надежности есть количественные характеристики способности, что составляют надежности системы.

Поскольку отказа и сбоев имеют случайный характер, то показатели надежности являются вероятностными величинами и при исследовании прибегают к методов, что используются в теории вероятности и математические статистике.

Наиболее распространенными количественными характеристиками надежности есть: вероятность безотказной работы в определенный интервал времени – $P(t)$; среднее наработки до первого отказа – $T_{СР}$; вероятность отказа – $Q(t)$; наработки на отказ – $t_{СР}$; частота отказов – $a(t)$; интенсивность отказов – $\lambda(t)$; параметр потока отказов – $\omega(t)$; функция готовности – Kг(t); коэффициент готовности – Kг.

Выбор количественных характеристик надежности зависит от вида объекта исследования – восстанавливаемого или невосстанавливаемого.

Возобновляемыми называют объекты, которые допускают ремонт в процессе выполнения своих функций. При отказе такие объекты прекращают функционирования только на период устранения отказа. Не возобновляемые объекты в процессе выполнения своих функций не допускают ремонта.

Следует отметить, что большинство элементов (компонентов) ИС СН построены по микросхемной технологии, поэтому ее ремонт (микросхемы) невозможен, а соответственно объекты – не возобновляемые.

Кроме того, в нашем исследовании область ограничивается оперированием только обобщенной надежностью, которая является составной кибернетической устойчивости. Поэтому в дальнейшем исследовании расчет составляющих надежности мы упускаем, путем введением выше указанного ограничения.

Для выяснения существующих подходов, методов и методик диагностирование кибернетической надежности информационной системы специального назначение осуществим поиск в открытых источниках информации по ключевым словами «подходы, методы и методики диагностирование кибернетической надежности функционирования информационной системы специального назначение».

Установлено, что в открытых научных источниках [7; 21; 22; 3] упоминается кибернадежность, как составляющая расчетной формулы киберустойчивости.

Следует отметить, что кибернадежность в методике оценки устойчивости функционирования объектов КИИ не рассчитывается, а принимается следующее предположение: техническая надежность за счет ряда специальных мероприятий по повышению оперативности устранения технических и программных отказов ТСОИ (например, за счет кластеризация серверов, резервирование средств с низкой надежностью компонентов ТСОИ) при своевременном и качественном проведении технического обслуживание считается приближенно малой, то есть $P_{ТН} = 1$.

Как свидетельствует современная практика, для обеспечение надежной работоспособности ИС применяют подход обновления ТСОИ до их предельных сроков наработки на отказ вследствие морального или физического старения.

Нельзя ограничиваться только физическим износом или старением некоторых объектов ИС. Для всех без исключения объектов ИС характерно моральное старение или экономическое старения. Под фактором морального старение понимается наступления события, когда заказчику, пользователю или тем, кто эксплуатирует ИС доступны объекты с лучшими характеристиками по показателю «цена/качество» или с лучшими функциональными возможностями, чем те, которые содержатся в данной системе. Фактор экономического старение имеет место тогда, когда экономически нецелесообразна дальнейшая эксплуатация любого объекта или группы объектов, или ИС в целом, хотя их физический износ еще не наступил и даже не скоро настанет. Для ИС типичная более высокая скорость морального старения в сравнению с экономическим, и тем более физическим старением или износом (см. рис. 1) [25, с. 22]. На этом рисунке приведены зависимости от времени показателей цена/качество (Ц/Я) в отношении морального старения (кривая $С_{МОР}(t)$), старения через экономическую нецелесообразность дальнейшей эксплуатации объекта (кривая $С_{ЭКОН}(t)$), физического старения или износа (кривая $С_{ФИЗ}(t)$).

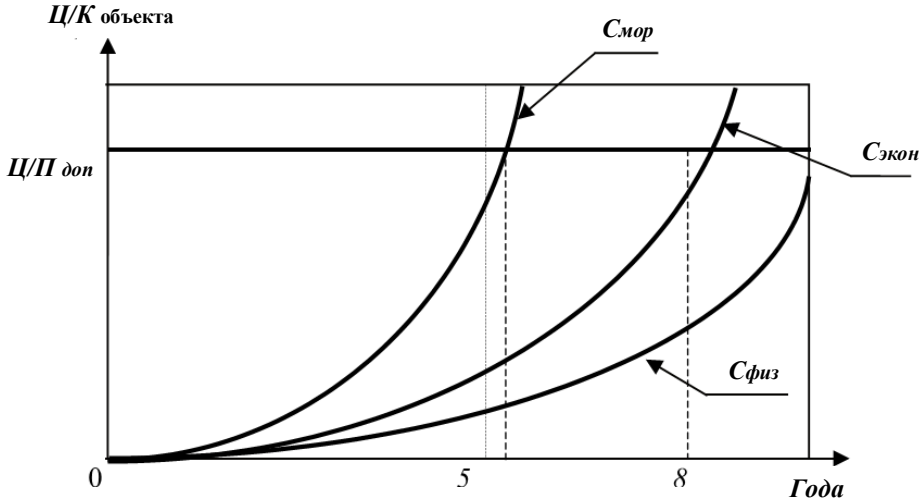

Рисунок 1 – Графики изменений скорости морального, экономической нецелесообразности или физического старения объекта ИС по критериям цена/качество (Ц/К) с учетом допустимого значения этого критерия

Эти зависимости носят качественный характер. Однако практика показывает, что уже через 5 лет эксплуатации, вследствие морального старения, целесообразно заменять ряд объектов ИС на более новые, хотя физическое старения или износ таких объектов далеки от предельного состояния. Это связано с тем, что кривая морального старения объекта пересекает и превышает предельно допустимый уровень показателя Ц/Я и, следовательно, дальнейшая его эксплуатация нерентабельна.

На рис.2, подано график кривой изменения интенсивности отказов средств в течение срока эксплуатации. Как практика показывает I фаза от 0 до t_1 имеет краткое промежуток времени, поэтому можно ею пренебречь. А за период от t_1 до t_2 превышает моральное старение.

Исходя из этого, авторы работы [3], также принимают ограничения, что $P_{\text{ТН}} = 1$, как и в работах [7; 21; 22] на аналогичных этапах в расчете объектов КИ Объединенной энергосистемы Украины. Тогда расчетная формула (1) примет упрощенного вида (2):

$$K_{\text{ОКИИ}^{\text{уо}}} = K_{\text{ОКИИ}^{\text{жив}}} \times K_{\text{ОКИИ}^{\text{пом}}} \quad (2)$$

Таким образом, анализ научной литературы по обеспечению кибернетической надежности ИС показал, что практически не рассмотрены вопросы, которые связанные с разработкой методов диагностирования кибернетической надежности в разных условиях их функционирования. Данное решение будет одной из частичных научных задач нашего исследования.

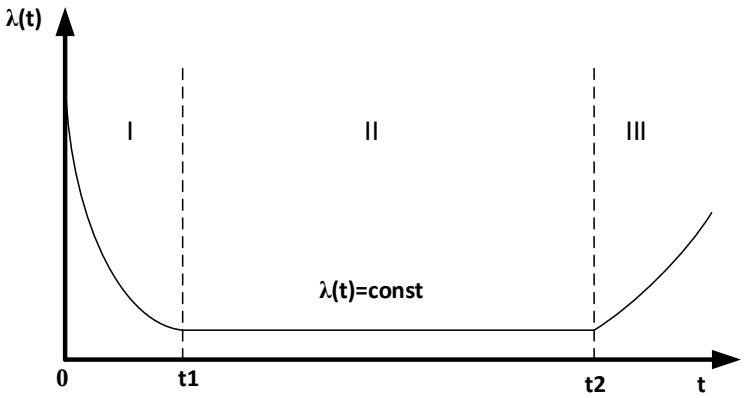

Рисунок 2 – График кривой изменения интенсивности отказов средств в течение срока эксплуатации

Проанализируем известные методы и методики диагностирование кибернетической живучести информационной системы специального назначения. Решение данной научной задачи начато с поиска в открытых источниках информации по ключевым словами «подходы, методы и методики диагностирование

кибернетической живучести функционирования информационной системы специального назначение».

В открытых научных источниках [7; 21; 22] упоминается киберживучесть, как составляющая киберустойчивости и рассчитывается на следующих этапах:

1.1 Оценка однозвенного объекта ИС.

Оценка киберживучести – предела состояний однозвенного объекта КИИ. $К_{ОКИИ}^{жил}$ – киберживучесть – живучесть объекта КИИ, трактуется как вероятность сохранение его работоспособности (выживание) в условиях выхода из строя технических средств обработки информации, то есть по сути – вклад каждого базового элемента однозвенного объекта КИИ в исполнение им целевой функции.

1.2. Оценка многозвенного объекта ИС. Оценка киберживучости – предела состояний многозвенного объекта ИС.

2. Этап оценка киберстойкости взаимодействующих объектов ИС (стволов объектов ИС).

Оценка киберживучести – пределл состояний ствола ИС.

3. Этап оценки киберстойкости ИС как сумма устойчивости ее элементов с учетом их коэффициента связности. Оценка киберживучасти ИС в целом, соответственно до текущего состояния стволов ИС и степенью важности, в данный момент времени, выполнения ими функций.

В указанной методике авторами работ [7; 21; 22] не приведены механизма диагностировании и расчетных соотношений.

Следует отметить, что авторы работы [3] позаимствовали наработки с научных работ [7; 21; 22] и в аналогичных этапах расчета киберживучести объектов КИ Объединенной энергосистемы Украины. Они также не приводят математический аппарат расчета.

Поскольку в расчетной формуле кибернетической устойчивости (1) содержится как кибернетическая составляющая живучесть, поэтому возникает необходимость в определении киберживучести.

Анализ проработанной научной литературы по вопросу кибернетической живучести показал, что практически не рассмотрены вопросы, которые связанные с разработкой методов диагностирования кибернетической живучести в информационных системах в различных условиях их функционирования в кибернетическом пространстве. Вычисления составляющей кибернетической живучести и диагностирование будет частичной научной задачей нашего диссертационного исследования.

Недостающий компонент в формуле (1) киберзащищенности предлагается получать по результатам его диагностирования по ранее разработанной методике [8; 18].

Постановка научного задачи на диссертационное исследования

Для обеспечения эффективного и бесперебойного функционирования информационной системы специального назначение в кибернетическом пространстве в условиях действий ДИВ определим приоритетные направления научного исследования:

усовершенствование нормативно-правовой базы в сфере кибернетической безопасности;

разработка и реализация адекватных организационных мероприятий;

разработка и применение комплексов и систем кибернетического защиты на принципах масштабирование и дополнения [16];

периодическое тестирование [9], обучение и аттестация штатного личного склада ответственного за эксплуатацию и обслуживание [15];

Как показывает практика, на сегодняшний день, ни одно из этих решений отдельно не может обеспечить необходим уровень защиты.

Поэтому, цель исследования должна заключаться в необходимости обосновании теоретических и практических основ ранней диагностики кибернетической устойчивости и ее настроек для обеспечения эффективного и бесперебойного функционирования информационной системы специального назначение в кибернетическом пространстве в условий неизбежных кибернетических действий ДИВ.

Это обеспечит повышение кибернетической безопасности и готовности ИС СН к выполнению поставленных задач без значительной потери активов на время восстановления.

В соответственно с выше рассмотренным нами определены основные задачи будущих исследований и их решения:

1. Анализ содержание понятия кибернетической устойчивости в научных исследованиях [6].

2. Обоснования методики диагностирование кибернетической устойчивости функционирования информационной системы специального назначение в кибернетическом пространстве [17; 29].

3. Обоснования методики расчета составляющих показателей кибернетической устойчивости функционирования информационной системы в кибернетическом пространстве.

4. Обоснования методики диагностирование кибернетической защищенности информационной системы с учетом ДИВ.

Перечисленные научные задачи исследования, их структурно-логический связь продемонстрировано на структурно-функциональной схеме, что одновременно определяет последовательность исследования и связь между результатным, представлены на рис.3.

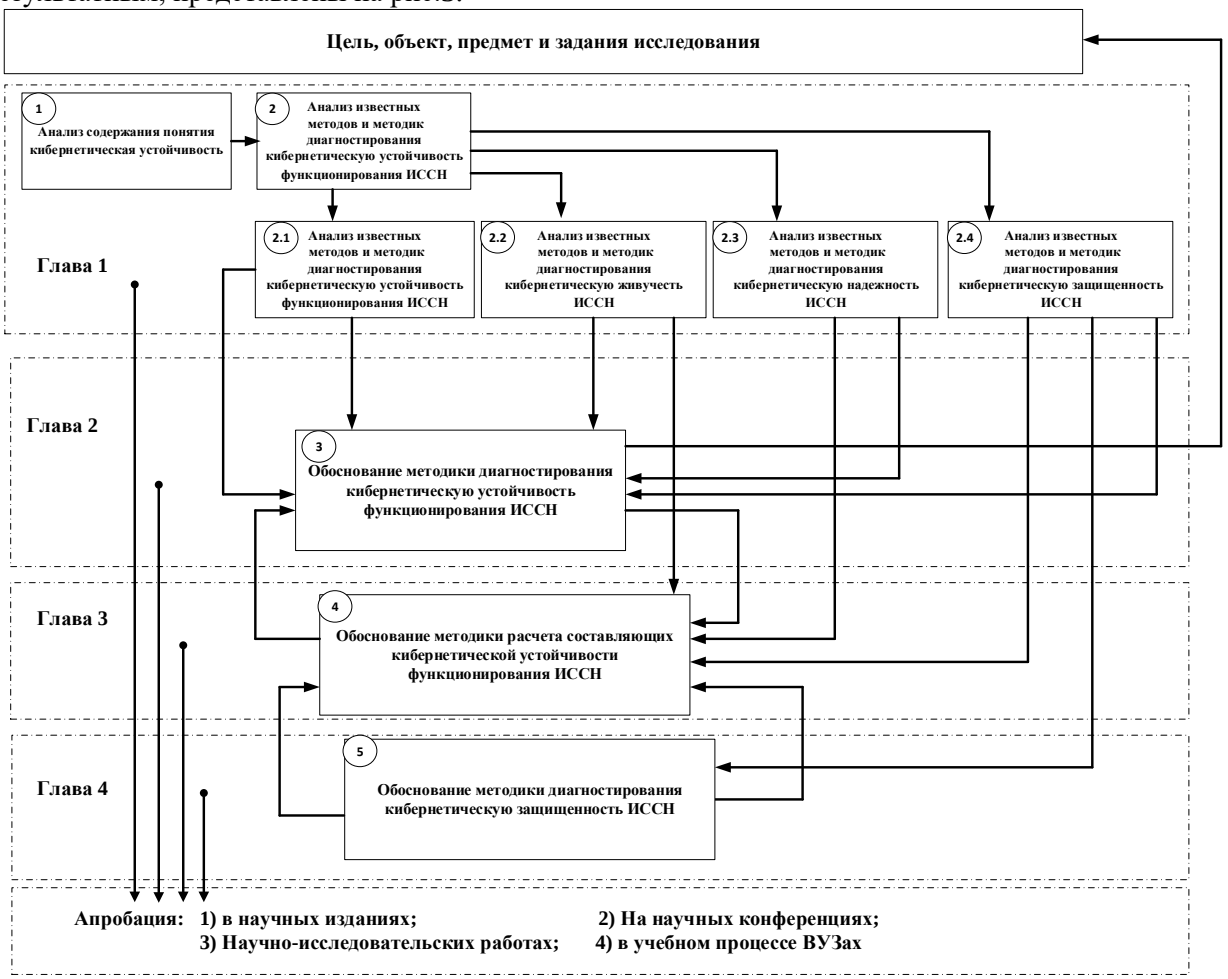

Рисунок 3 – Структурно-функциональная схема научного исследования

ВЫВОДЫ.

Важнейшими научными и практическими результатами являются:

1. Проанализированы известные методы и методики диагностирование кибернетической устойчивости функционирования ИС СН в кибернетическом пространстве. Установлено, что в настоящее время отсутствует методика диагностирование кибернетической устойчивости.

2. Таким образом, цель исследования должна заключаться в необходимости обоснования теоретических и практических основ ранней диагностики кибернетической устойчивости и ее настроек для обеспечения эффективного и бесперебойного функционирования информационной системы специального назначение в кибернетическом пространстве за неизбежных условий кибернетических действий деструктивных информационных воздействий.

3. Полученные научные результаты исследования является основанием к формированию научных задач на разработку методики диагностирование кибернетической устойчивости функционирования ИС СН в кибернетическом пространстве.

СПИСОК ЛИТЕРАТУРЫ

1. Боговик А.В., Игнатов В.В. Теория управления в системах военного назначения. СПб.: ВАС, 2008. 460 с.

2. Гибсон У. Нейромант: Фантастический роман / Пер. с англ. Е. Летова, М. Пчелинцева. М.: Аст; СПб.: Terra Fantastica, 2000. 317с.
3. Гончар С.Ф., Герасимов Р.П., Ткаченко В.В. Дослідження проблеми кіберживучості Об'єднаної енергосистеми України // Міжнародний науково-теоретичний журнал «Електронне моделювання». 2019. Т.41. №1. С. 43 – 54.
4. Давыдов А.Е., Савицкий О.К., Максимов Р.В. Защита и безопасность ведомственных интегрированных инфокоммуникационных систем. Москва: Воентелеком, 2015. 520 с.
5. Даник Ю.Г. Вдовенко С.Г. Ланцюгові ефекти в кібердіях // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. К.: ВІКНУ, 2019. № 64. С. 71 – 90.
6. Забара С.С., Хлапонин Ю.И., Козубцова Л.М. Анализ понятия кибернетической стойкости информационной системы специального назначения // Materials of the XVI International scientific and practical Conference Science without borders – 2020 (March 30 – April 7, 2020): Sheffield. Science and education LTD. Pp. 20 – 23. ISBN 978-966-8736-05-6.
7. Захарченко Р.И., Королев И.Д. Методика оценки устойчивости функционирования объектов критической информационной инфраструктуры функционирующей в киберпространстве // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10. № 2. С. 52 – 61.
8. Козубцов І.М., Козубцова Л.М., Куцаєв В.В., Терещенко Т.П. Методика оцінки кібернетичної захищеності системи зв'язку організації // Сучасні інформаційні технології у сфері безпеки та оборони. 2018. №1 (31). С. 43 – 46.
9. Козубцов І.М., Козубцова Л.М., Куцаєв В.В., Терещенко Т.П. Стратегічні напрямки анкетування спеціалістів інформаційної та кібернетичної безпеки для з'ясування рівня кібернетичної захищеності організації // Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 30 березня 2018 р.). К.: Нац. акад. СБУ, 2018. С. 89 – 91.
10. Козубцов І.М., Козубцова Л.М., Куцаєв В.В., Терещенко Т.П., Штонда Р.М, Черноног О.О. Обґрунтування поняття терміну глобального колапсу інформаційно-телекомунікаційних систем // Міжнародна науково-практична конференція "Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку" (15 березня 2019 року, м. Харків). Харків. Національна академія Національної гвардії України, 2019. С. 57 – 59.
11. Козубцов І.М., Козубцова Л.М., Терещенко Т.П., Куцаєв В.В. Глобальний колапс інформаційно-телекомунікаційних систем в наслідок порушення роботи сучасних інформаційних технологій у секторі безпеки і оборони // Міжнародна науково-практична конференція «Спільні дії військових формувань і правоохоронних органів держави: проблеми та перспективи» (м. Одеса 12-13 вересня 2019 р.). Одеса. Військова академія, 2019. С. 229 – 230.
12. Козубцов І.М., Куцаєв В.В. Філософія інформаційної безпеки в умовах її кібернетичного розповсюдження в сучасної динамічній наукової картині світу на прикладі надання знань молодим вченим та студентам // Гілея: науковий вісник. Збірник наукових праць. К.: ВІР УАН, 2013. Вип. 73(№6). С. 291 – 293.
13. Козубцов І.М., Куцаєв В.В., Козубцова Л.М., Терещенко Т.П. Кібернетичні атаки як механізм створення штучного глобального колапсу інформаційно-телекомунікаційних систем // Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 4 квітня 2019 р.). К.: Нац. акад. СБУ, 2019. С.221 – 223.
14. Козубцов І.М., Куцаєв В.В., Козубцова Л.М., Терещенко Т.П. Тлумачення терміну "кібернетична безпека" через призму кібернетики // Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 4 квітня 2019 р.). К.: Нац. акад. СБУ, 2019. С.219 – 221.
15. Козубцов І.М., Куцаєв В.В., Срібний С.П. Концепція нового підходу до підготовки фахівців з інформаційною безпекою // Актуальні проблеми управління інформаційною безпекою держави : зб. матеріалів науково-практичної конференції (Київ, 20 березня 2014 року): у 2 ч. Ч.1. К.: Центр навч.-наук. та наук-практ. вид. НА СБ України, 2014. С. 170 – 175.
16. Козубцов І.М., Куцаєв В.В., Ткач В.О., Козубцова Л.М. Концептуальний підхід до побудови системи кібернетичної безпеки стаціонарних інформаційно-телекомунікаційних вузлів України на принципах масштабування та доповнення // Науково-практичний журнал. Сучасні інформаційні технології у сфері безпеки та оборони. Національний університет оборони України. 2015. №3(24) С.

47 – 55.

17. Козубцова Л.М. Апробація структури методики діагностування кібернетичної стійкості функціонування інформаційної системи спеціального призначення в кібернетичному просторі // Міжнародна науково-практична конференція “Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку” (17 березня 2020 року, м. Харків). Харків. Національна академія Національної гвардії України, 2020. С. 141 – 142.
18. Куцаєв В.В., Радченко М.М., Козубцова Л.М. Методика оцінки кібернетичної захищеності інформаційно-телекомунікаційного вузла зв’язку // Збірник наукових праць ВІТІ. К.: ВІТІ, 2018. № 2. С. 67 – 76.
19. Ложков А.В. Методика оценки надежности вычислительной сети // Научные записки молодых исследователей. 2014. № 4. С. 28 – 31.
20. Мараховський Л.Ф., Козубцов І.М. Філософія формування цілісної динамічної наукової картини світу знань : реалізація ідеї академіка Володимира Івановича Вернадського // Філософський журнал Донецького національного технічного університету „Ноосфера і цивілізація”. 2013. Вип. 1(14). С. 108 – 116.
21. Минаев В.А., Королев И.Д., Зеленцова Е.В., Захарченко Р.И. Критическая информационная инфраструктура: оценка устойчивости функционирования // Радиопромышленность. 2018. Т. 28. №4. С. 59 – 67.
22.] Минаев В.А., Крупенин А.В., Королев И.Д., Бондарь К.М., Захарченко Р.И. Оценка устойчивости функционирования критической информационной инфраструктуры // «Вестник РосНОУ», серия «Сложные системы: модели, анализ и управление». 2018. Выпуск 4. Информатика и вычислительная техника. С. 129 – 138.
23. Моисеев В.С., Козар А.Н., Дятчин В.В. Информационная безопасность автоматизированных систем управления специального назначения: Монография. Казань. Казанское высшее артиллерийское командное училище (военный институт) имени маршала артиллерии М.Н. Чистякова, 2006. – 384 с.
24. Слипченко В.И. Войны шестого поколения оружие и военное искусство будущего. М.: Вече, 2002. 382 с.
25. Шубинский И.Б. Структурная надежность информационных систем. Методы анализа. М.: «Журнал Надежность», 2012. 216 с.
26. Шубинский И.Б. Функциональная надежность информационных систем. Методы анализа. М.: «Журнал Надежность», 2012, 296 с.
27. Department of Defense Instruction. Number 8530.01, March 7, 2016 “Cybersecurity Activities Support to DoD Information Network Operations”. 44 p. https://apps.dtic.mil/dtic/tr/fulltext/u2/1005132.pdf.
28. Department of Defense Instruction. Number 8530.01, March 7, 2016, Incorporating Change 1, July 25, 2017.“Cybersecurity Activities Support to DoD Information Network Operations”. 45 p. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/853001p.pdf.
29. Zabara S., Khlaponin Yu., Kozubtsova L. Methods for diagnosing cybernetic stability of a special purpose information system // Scientific and Practical Cyber Security Journal (SPCSJ). 2020. Vol. 4(1). Pp. 80 – 86 ISSN 2587-4667 Scientific Cyber Security Association (SCSA). URL: https://journal.scsa.ge/wp-content/uploads/2020/04/10-41-spcsj.pdf.