ИНФОРМАЦИОННАЯ ЖИВУЧЕСТЬ КОРАБЛЯ, СУДНА: ПРИКЛАДНАЯ ТЕОРИЯ ОБЕСПЕЧЕНИЯ ВОЕННО-ТЕХНОЛОГИЧЕСКОГО ПРЕВОСХОДСТВА

Алексеев А. В.[1], Дригола В. К.[2], Михальчук А. В.[3]

DOI:10.21681/3034-4050-2025-4-79-89

Ключевые слова: *целеполагание; модель; живучесть судна; мониторинг; валидный контроль; уязвимость; угроза; конфиденциальность; доступность; целостность.*

Аннотация

Цель работы *состоит в обосновании необходимости расширения понятия живучести корабля, судна и разработке основных положений прикладной теории информационной живучести корабля, судна (И ЖС) в обеспечение военно-технологического превосходства.*

Метод исследования: *систематизация данных анализа, синтеза и оптимизации ИЖС на основе квалиметрической оценки агрегированного показателя проектного качества и эффективности эксплуатации системы комплексной защиты информации (СКЗИ) в составе автоматизированной системы обработки информации в защищенном исполнении (АСЗИ).*

Результаты исследования: *приведены типовые структурные модели ИЖС, СКЗИ, вербальная модель уязвимостей и угроз ИЖС, комплексная математическая модель оценки и оптимизации ИЖС, структурно-информационная модель цифрового двойника СКЗИ и пример программной реализации в варианте роботизированного проектного комплекса «КАСОР-24.4», обобщены полученные результаты формирования прикладной теории ИЖС.*

Научная новизна и практическая ценность *исследования состоит в обобщение и развитие прикладных теоретических аспектов введения и модельного представления анализа, синтеза и оптимизации нового для судостроительной отрасли понятия «информационная живучесть корабля, судна». Это позволило расширить категорию живучесть судна и впервые количественно учитывать/цифровизовать такие актуальные сегодня факторы развития информационных технологий как защищенность информационных ресурсов корабля, судна, их конфиденциальность, доступность, целостность при обеспечение военно-научно-технологического превосходства над потенциальным противником.*

Введение

Среди современных системных категорий и свойств судов, как основного класса объектов морской техники и морской инфраструктуры (ОМТИ), продолжает оставаться и является важнейшим понятие ***живучести судна (ЖС)***, введенное в 1894 г. в теорию и практику судостроения адмиралом С.О. Макаровым.

Регламентированное в том числе наставлениями по борьбе за живучесть кораблей (ВМФ), морских и речных судов (таможенных органов РФ) понятие ЖС определяется сегодня как способность противостоять последствиям аварийных повреждений, возникновению и распространению пожаров, возникновению взрывов и радиационных заражений, сохранять, восстанавливать и поддерживать при этом в достаточной мере свои мореходные качества и обеспечивать безопасность находящихся на его борту людей, сохранность грузов и судового имущества [1]. В общем случае ЖС обеспечивается и определяется (ГОСТ 27.002-2015) следующими его свойствами: непотопляемостью (Н), взрыво-пожаро-радиационной безопасностью (ВПРБ), живучестью технических средств и оружия (ЖТС), защищенностью и подготовленностью экипажа судна к борьбе за ЖС (ЗЭ), устойчивостью системы управления ЖС (УСУ) [2].

1 Алексеев Анатолий Владимирович, доктор технических наук, профессор, профессор кафедры судовой автоматики и измерений Санкт-Петербургского государственного морского технического университета, г. Санкт-Петербург, Россия. E-mail: iapbgks@bk.ru

2 Дригола Владимир Кириллович, кандидат военных наук, старший научный сотрудник Военного учебно-научного центра ВМФ «Военно-морская академия им. Н. Г. Кузнецова», г. Санкт-Петербург, Россия. E-mail: velena.spb@mail.ru

3 Михальчук Андрей Васильевич, кандидат технических наук, доцент кафедры судовой автоматики и измерений Санкт-Петербургского государственного морского технического университета, г. Санкт-Петербург, Россия. E-mail: 335mav@mail.ru

Постановка задачи

Живучесть (survivability) в соответствии с определением профессора Рябинина И. А. рассматривается как способность системы сохранять свойства, необходимые для выполнения заданного назначения при форс-мажорных поражающих воздействиях, не предусмотренных условиями нормальной эксплуатации, т.е. при взрывах, пожарах, затоплениях и прочих факторах, которые сегодня могут и должны быть расширены ***информационными факторами и угрозами живучести корабля, судна (ИФЖ)*** типа:

1. Угрозы несовершенства проектных решений/средств и систем защиты информации (СЗИ), организации, управления и нарушения регламентов комплексной защиты информации (КЗИ), угрозы физических атак и нанесения ущерба судовым информационным ресурсам (ИР) на отчуждаемых и встроенных носителях информации долговременного хранения, на средствах обработки и хранения оперативной информации, на средствах (портах) ввода / вывода информации.
2. Угрозы конфиденциальности информации (неправомерного / несанкционированного доступа, блокирования, утечки, потери, перехвата, съема, копирования, хищения, разглашения, компрометации информации.
3. Угрозы доступности информации вследствие воздействия вредоносных кодов (вирусы, черви, троянские программы, спам, фишинг), DDoS-атак, ….
4. Угрозы целостности информации (модификация данных, деструктивные воздействия / уничтожение / утрата.
5. Антропогенные угрозы (недостаточная квалификация и ошибки операторов, экипажа, инсайдеры, хакерские атаки / групповые атаки, утечка информации от экипажа, социальная инженерия
6. Техногенные угрозы (отказы оборудования и программного обеспечения (уязвимости операционных систем, сетевых протоколов, программных приложений, программные закладки) аварии и аварийные ситуации.
7. Угрозы форс-мажорных обстоятельств / ситуаций (природные катастрофы, затопление, пожары, взрывы, радиационная активность).

В этой связи встает актуальная научно-методическая и организационная задача определения роли и места, прикладной теории обеспечения ***информационной живучести судна (ИЖС***, информационной безопасности судна и ОМТИ в целом) при *обеспечении* ***военно-технологического информационного превосходства*** (ВТПи) над противником в ряду основных факторов, показателей и технологий обеспечения ЖС, ВТП в целом.

Решение поставленной задачи

Живучесть как одно из важнейших свойств корабля, судна развивается и совершенствуется на протяжении всего исторического опыта судостроения и эксплуатации кораблей, судов. В этой связи расширение понятия ЖС с учетом специфики этапа современного технологического развития следует рассматривать как вполне естественное в условиях цифровой трансформации личности, общества, государства на базе интенсивного развития современных информационных технологий.

Введение понятия ИЖС в контексте [1–4] позволяет учитывать ***основные тенденции современного развития кораблей, судов***:

- интеллектуализацию управления за счет совершенствования алгоритмов, автоматизации процессов обоснования проектных решений, поддержки принятия и регистрации решений, визуализации, мониторинга и автоматического контроля их исполнения, использования элементов искусственного интеллекта [2–12];
- усложнение информационно-управляющих и роботизированных систем путем наращивания функционала, интеграции средств и подсистем [2, 3];
- комплексную интеграцию систем управления с соответствующим укрупнением и исключением рабочих мест операторов нижестоящих уровней и контуров управления [3–5];
- переход на дистанционное, распределенное и роботизированное управление отдельными судовыми системами и судном в целом [9–10].

При этом статистика международных инцидентов демонстрирует ***устойчивый рост кибератак на морскую инфраструктуру***. Только за последние три года зафиксировано более 400 значимых киберинцидентов в морском секторе, что на 67 % превышает показатели предыдущего трехлетнего периода [11].

Рис. 1. Возможные варианты судовых информационных инцидентов

Рис. 2. TOP-21 событий и фактов противоборства в информационной сфере

С учетом возрастания политической нестабильности в ряде регионов перспективными инцидентами в части воздействия на морские суда могут быть (рис. 1) действия по блокировке (отключению), перехвату управления судовыми системами, блокировка обмена данными и пр.

Реализация указанных инцидентов будет направлена на нанесение ущерба путем создания аварийных ситуаций, перетекающих в аварии различного характера и аварийные ситуации.

Международными и государственными стандартами определены системные требования к информационной безопасности судна, однако, инциденты, связанные с воздействием на информационные системы, сегодня не трактуются как аварийные ситуации.

По мнению авторов, с учетом возможных последствий нарушения информационной безопасности (ИБ) судна, ***все инциденты ИБ следует рассматривать как аварийные ситуации***, а их своевременное предотвращение и безусловное устранение должно осуществляться в рамках такого важного элемента борьбы за живучесть как информационная живучесть судна.

Обуславливается это тем, что наносимый при этом ущерб, как показывает анализ исторических примеров обеспечения информационного превосходства в информационной сфере (рис. 2 [10]), может ***существенно превосходить*** стоимость самих судов и грузов, причем, во много раз, включая человеческие жертвы.

В обеспечение развития прикладной теории ИЖС ***понятие ИЖС*** в контексте [2, 3, 12] предлагается рассматривать как способность корабля, судна *обеспечивать постоянную готовность к действиям* по прямому назначению, способность сохранять и восстанавливать свои свойства *при* ***информационных инцидентах*** **(ИнИ)**, а также *готовность противостоять* последствиям ИнИ, воздействию атак, *сохранять и восстанавливать* при этом в достаточной мере управляемость судна и *обеспечивать безопасность* находящихся на борту судна пассажиров и экипажа, сохранность грузов и судового имущества.

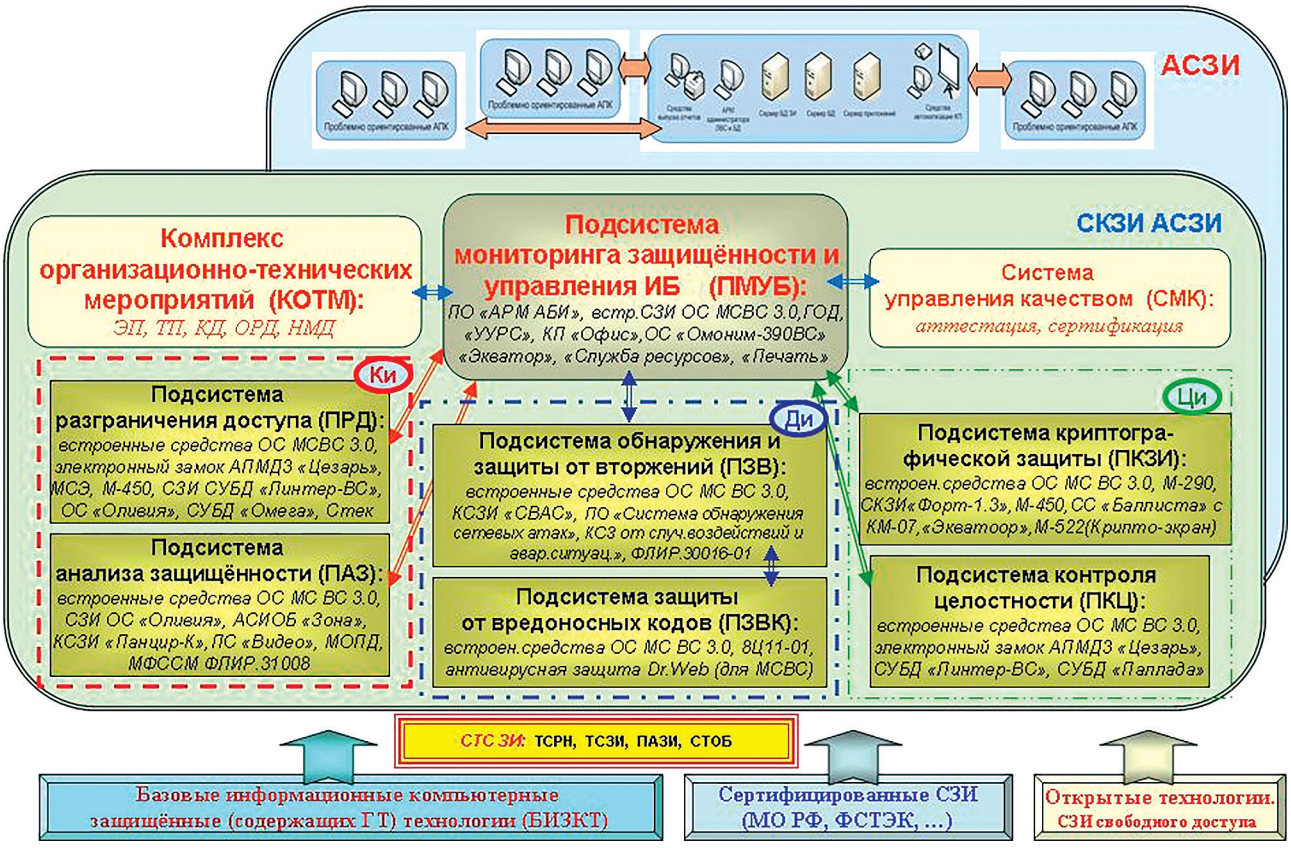

Рис. 3. Типовая архитектура и технологии СКЗИ в составе АСЗИ типового ОМТИ с наиболее характерными представителями подсистем защиты информации

Под ***борьбой за ИЖС*** предлагается понимать своевременные энергичные, инициативные и квалифицированные действия его экипажа *по обеспечению*:

- проектного качества и эффективности эксплуатации ***системы комплексной защиты информации*** **(СКЗИ)** в составе судовой ***автоматизированной системы в защищенном исполнении*** **(АСЗИ)**, типовая структурная модель которой приведена на рис. 3 [8–10];
- конфиденциальности, доступности, целостности ***информационных ресурсов*** **(ИР)** судна и ИБ в целом;
  предупреждению возникновения и неуправляемого развития ИнИ, а также – по поддержанию в постоянной готовности к действию ***информационно-коммуникационных*** **(ИКС)** и ***информационно-управляющих средств и систем*** судна **(ИУС)**.

Требования к организации обеспечения информационной живучести судна

Борьба за ИЖС должна быть отработанной на тренировках и учениях обязанностью всех членов экипажа, а также регламентироваться Уставом службы на судах, Наставлением по борьбе за живучесть судов (НБЖС, ЦНИИМФ, 2004) и документами по Системе управления безопасностью (СУБ) судна, требованиями Международного кодекса по управлению безопасностью (МКУБ) [2, 3].

Отработка организации борьбы за ИЖС должна быть составной частью повседневной службы на судне и направлена на рациональное распределение членов экипажа в интересах эффективного использования стационарных и мобильных ИКС и ИУС при ИнИ, воздействии атак и вторжений как в портах, включая иностранные, так и на переходе морем.

ИЖС включает в себя ряд *организационно-технических мероприятий* по следующим направлениям:

- готовность СКЗИ в составе судовых АСЗИ к действиям по прямому назначению с обеспечением научно-технологического и военно-технологического превосходства по критерию $\text{ВТП} = Q / Q_{\text{П}}$, где Q – агрегированный (обобщенный, интегрированный, системный, адмиральский) показатель проектного качества/эффективности эксплуатации СКЗИ в составе АСЗИ, а $Q_{\text{П}}$ – аналогичный показатель для СКЗИ потенциального противника с прогнозируемыми по данным разведки и военно-научной экспертизы характеристиками, оцениваемые по алгоритмам, приведенным в [8–10];
- своевременное выявление уязвимостей, угроз и информационных воздействий (ИВ) с их классификацией, идентификацией и оценкой возможностей по нанесению ущерба;
- сохранение и восстановление функциональных свойств систем (комплексов) судна за счет отработанных и слаженных действий экипажа по эффективному использованию СКЗИ;
- устранение последствий информационных инцидентов и их всевозможных проявлений;
- военно-научный анализ и прогнозирование возможных аварий по результатам реализации киберугроз, в том числе представленных на рис. 4.

Рис. 4. Типовой характер возможных аварий по результатам реализации киберугроз

Структура

В этой связи особое внимание при разработке и эксплуатации объектов морской техники и инфраструктуры сегодня следует уделять СКЗИ, как одному из ключевых элементов АСЗИ, в состав которой согласно рис. 3, как правило, входят следующие подсистемы [2, 3]:

1. **Подсистема мониторинга, прогнозирования, контроля и управления ИЖС (ПМУБ)**, реализуемая сегодня средствами защиты информации корабля, судна типа 4789.ИАСЗИ ГК, 4451.DATAPK, 2720.Dallas Lock 8.0-K (цифры в сокращенном название средств означают номер сертификата в Государственном реестре сертифицированных средств ФСТЭК РФ).

2. **Подсистема разграничения доступа к информационным ресурсам (ИР) корабля, судна (ПРД)**, реализуемая сегодня средствами типа 4795.ПО «Реестр РВК», 3474.ARMlock, 4792.ПО СА СЦ ЭП.

3. **Подсистема криптографической защиты ИР (ПКЗИ)** корабля, судна, реализуемые сегодня средствами типа 4268. Континент-СОВ.4, 4125.АПК «VPN/FW ЗАСТАВА-150», 4145.АПКШ Континент.3.9.

4. **Подсистема обнаружения и защиты от вторжений в ИР (ПЗВ)** корабля, судна, реализуемая сегодня средствами защиты информации от вторжений типа 4042.СОПВ PosTechnNetAttDiscovery, 4759.Реализация ГОЗ, 3597.ЭЗ «Витязь 2.2».

5. **Подсистема оценки, мониторинга, анализа и контроля защищенности ИР корабля, судна (ПАЗ)**, реализуемая сегодня средствами типа 4451.ПК ОМ ИБиЗ «DATAPK», 4159.СМИБ SIEM, 4574.Security Vision ЦИМУ ИБ.

6. **Подсистема контроля целостности ИР корабля в составе соединения (ПКЦ)**, реализуемая сегодня средствами типа 2557.ОС СН Astra Linux Special Edition, 4742.ГосКонтроль, 4293.АИТ «АИСТ-С».

7. **Подсистема защиты ИР корабля, судна от вредоносных (вирусов, спама, фишинга и т.п.) кодов (ПЗВК)**, реализуемая сегодня средствами типа 3676.Kaspersky Security 9.0 Exchange Servers, 2840.Kaspersky Security 8.0, 4604.Positive Technologies Sandbox.

8. **Комплекс организационно-технических мероприятий по обеспечению ИЖС корабля, судна (КОТМ)**, по управлению проектным качеством и эффективностью (мерой практической реализации проектного качества) подсистемы ИЖС, включая мероприятия по контролю, оценке технической готовности судна [9–10], реализуемые сегодня регламентами типа «Положение о Службе ИБ НИЦ СПбЭТУ», «Положение о КИС АО «Концерн «МПО «ГидроПрибор», «Политика в области ИБ № ПЗ-11.01 П-01 в.2.00», РосНефть [10].

9. **Система менеджмента качества обеспечения ИБ корабля, судна (СМИБ)**, реализуемая сегодня регламентами и средствами типа «Программный комплекс мониторинга качества вооружений, военной и специальной техники «ПК СМК ВВСТ», «Русский Регистр. Системы МК ИБ», «Система менеджмента качества. Стандарт организации. СТО 6.5-1. Политика информационной безопасности».

При этом ***типовыми моделями тактических уязвимостей*** (существующих дефектов построения, функционирования и использования АСЗИ в части ИЖС) и соответствующих ***информационно-тактических угроз ИЖК*** (ИТУ, потенциальных событий по реализации уязвимостей, нарушению регламентов обработки информации) следует считать:

ИТУ-1: Возможность потери военно-технологического превосходства над потенциальным противником в следствие **негативного влияния субъективных свойств членов экипажа** (**ЧФ**, «человеческий фактор»). Угроза ЧФ может быть обусловлена недостаточной подготовкой (знаниями, навыками, способностями, опытом) и соответствующими ошибками эксплуатации, ограниченной мотивируемостью (безинициативностью, безответственностью) и нелояльностью (злоупотреблением должностным положением) членов экипажа и т.п.

ИТУ-2: Киберсетевые воздействия (КСВ), осуществляемые установленными/неустановленными субъектами информационного взаимодействия по информационно-коммуникационным каналам. Угроза КСВ реализуется с использованием средств разведки (включая технический шпионаж), средств противодействия, формирования напряженной и ложной обстановки, провоцирования экипажа на нерациональные действия, шантажа, заражения вредоносными кодами с деструктивными функциями, спама и т.п.

ИТУ-3: Технологические угрозы (ТУгр), обусловленные спецификой программно-аппаратных средств и процессов (включая «зависания» программного обеспечения, потеря целостности и доступности данных).

Рис. 5. Комплексная математическая модель оценки и оптимизации ИЖС

ИТУ-4: Угрозы рефлексивного воздействия (УРВ), обусловленные формированием установленными и/или неустановленными субъектами информационного взаимодействия «целевой» обстановки в информационной среде в интересах рефлексивного управления членами экипажа, кораблем и соединением кораблей в целом.

ИТУ-5: Другие возможные и ранее не идентифицированные угрозы (**ДрУ**), обусловленные интенсивным развитием информационных технологий, включая искусственный интеллект, роботизацию управления.

В обеспечение прикладной теории ИЖС модельное представление процессов и качества создаваемых систем обеспечения ИЖС и управления мероприятиями по ее обеспечению, по нашему мнению, прежде всего целесообразно использовать **Полимодельный квалиметрический метод системной оптимизации** [2, 3] и соответствующую ***аналитическую модель***, приведенную на рис. 5 [10].

Реализация прикладной теории

Парадигма обеспечения ИЖС, по мнению авторов, должна включать системообразующую идею проектного обоснования, оптимизации, мониторинга и прогнозирования свойств **комплексных судовых систем** защиты информации с учетом всего множества системных критериев и показателей проектного качества. В настоящее время группой специалистов СПбГМТУ разработан и используется в исследованиях вопросов ИЖС Роботизированный проектный комплекс (РПК) «КАСОР-24» [8–10], экранная форма приведена на рис. 6.

Преимуществом РПК является возможность моделирования и исследования свойств комплексных систем обеспечения ИЖС с цифровой оценкой, как показано на рис. 6 агрегированного показателя качества СКЗИ (значение АПК = 80,5 %) и соответствующих значений конфиденциальности ИР (К = 77,9 %), доступности (Д = 80,9 %), целостности (Ц = 82,6 %). А также реализованы возможности технологии цифрового двойника СКЗИ, как цифровой модели СКЗИ в составе АСЗИ с режимами функционирования «1.ЦП» (цифровой паспорт), «2.ЦМ» (цифровая модель, с вводом сценарных исходных данных), «3.ЦТ» (цифровая тень, с вводом исходных данных с реального объекта типа СКЗИ).

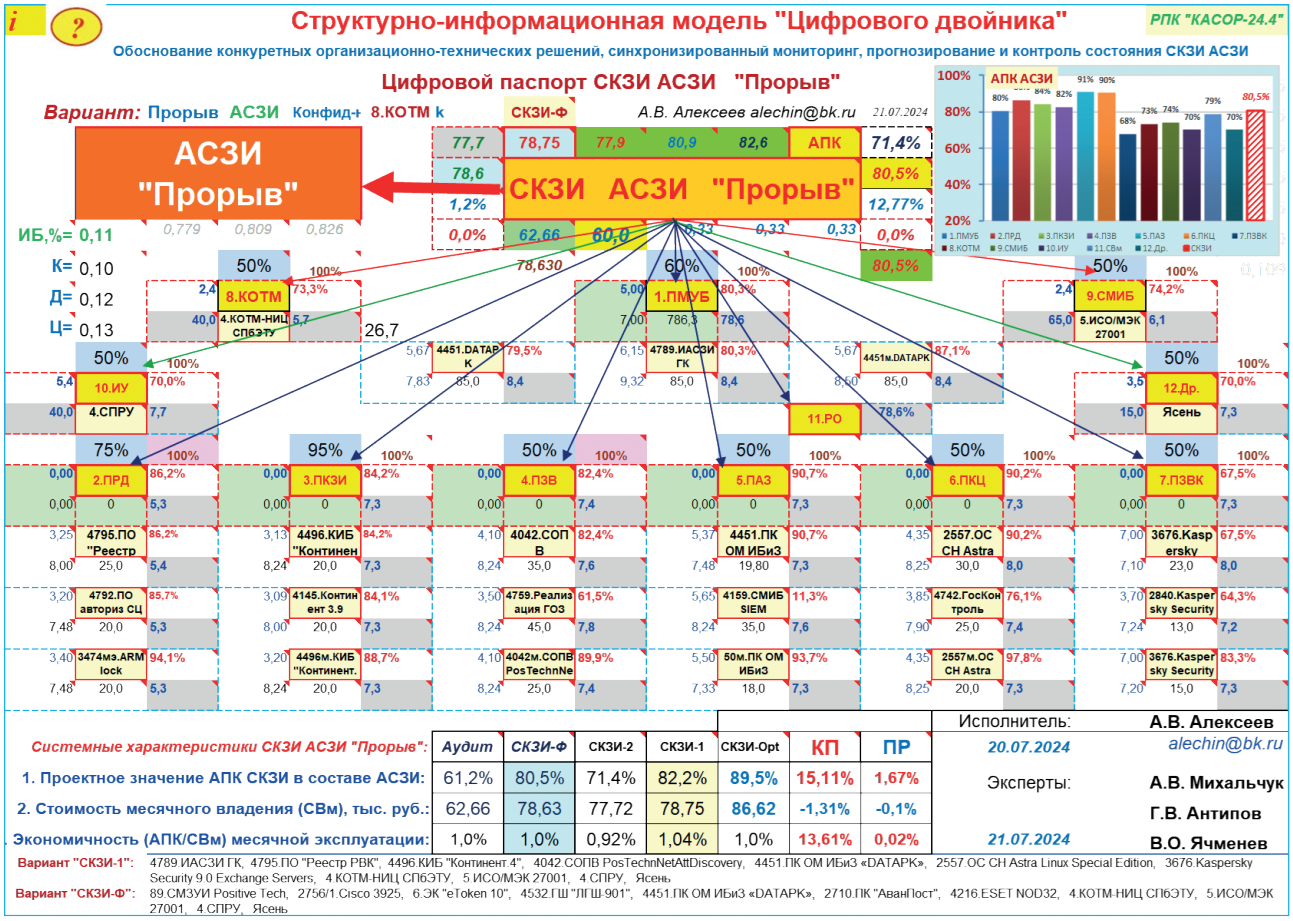

Рис. 6. Структурно-информационная модель «Цифрового двойника» (экранная форма РПК)

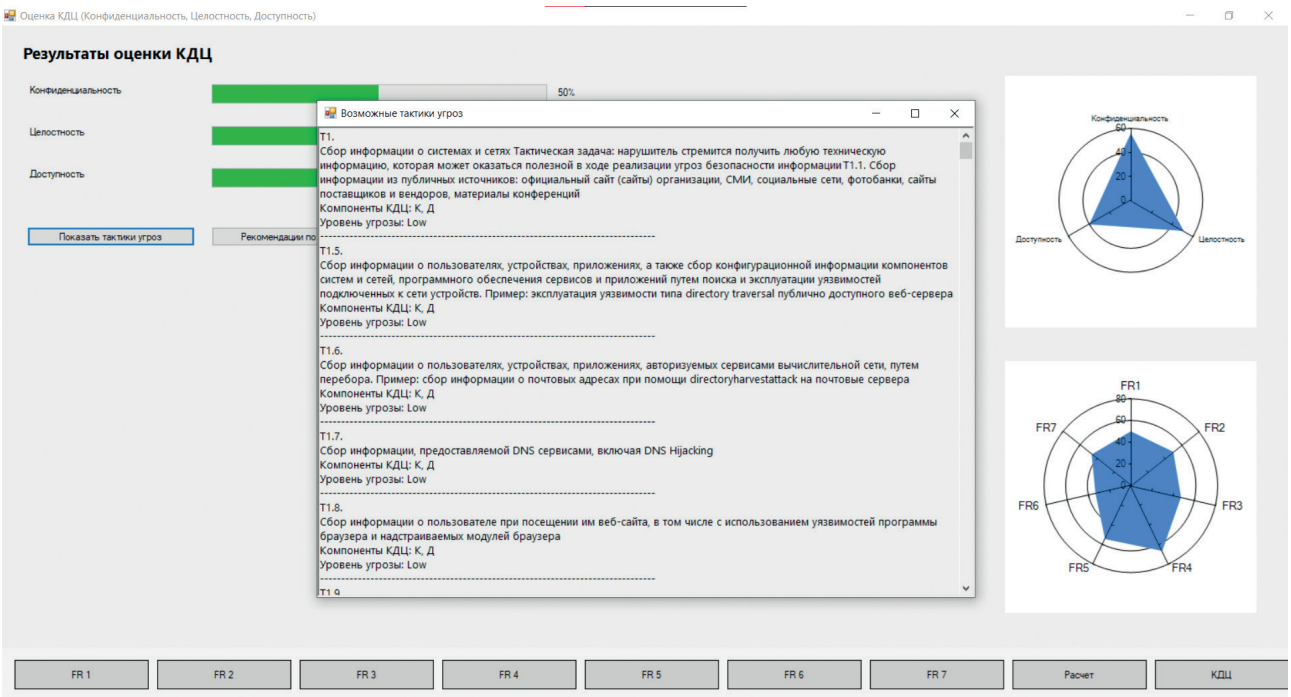

Рис. 7. Пример экранной формы ПК ИЖС (в части контроля ФТ и СТ)

Апробация

В рамках научно-исследовательских и выпускных квалификационных работ уже сегодня студентами СПбГМТУ [8] РПК используется при обосновании мер КЗИ и разрабатываются программные комплексы цифровой оценки проектного качества ИЖС, ожидаемой эффективности частных мероприятий по обеспечению ИЖС, например, при контроле реализации названных в РМРС «фундаментальными требованиями» (ФТ, конфиденциальности, доступности, целостности) и системных требований (СТ, комплексной защиты информации/информационной безопасности, военно-технологического превосходства) корабля, судна (рис. 7) с учетом соответствующих тактик, используемых для построения сценариев реализации угроз безопасности информации корабля, судна.

Заключение

Проведенные исследования по разработке прикладной теории ИЖС в обеспечение научно-технологического превосходства в информационной сфере, приведенные результаты анализа и систематизации вопросов формирования понятия «информационная живучесть корабля, судна» (ИЖС) и практические аспекты решения системной проблемы обеспечения информационного превосходства в управлении ИЖС на базе анализа технологических решений максимизации ИЖС типовых объектов морской техники и морской инфраструктуры показали, что:

- сегодня первостепенное значение имеют вопросы **системного управления ЖС** по традиционным критериям оперативности, достоверности используемых данных, устойчивости, скрытности, непрерывности, ресурсной обеспеченности с соответствующими частными показателями качества типа работное время решения комплекса функциональных задач, адекватность используемых данных;
- при необходимости одновременной оценки, мониторинга и контроля критически важных показателей комплексной защищенности ИР корабля, их соединений, судна в составе флота, конфиденциальности, доступности, целостности информационных ресурсов;
- а также необходимости перехода к метасистемному цифровому анализу и синтезу киберустойчивости СКЗИ в составе АСЗИ корабля, судна, рефлексивности и ментальности управления, его имитоскрытности, эргогномичности.

Показано, что обеспечение ИЖС ОМТИ в условиях интенсивного информационно-технологического развития является *сложнейшей и высоко востребованной задачей* целеполагания, роботизированного управления с использованием технологий полимодельного мониторинга, анализа, синтеза и оптимизации управленческих решений с мониторингом контроля их реализации по технологии цифровых двойников, адаптивной корректировки, верификации и валидного контроля.

Приведенные теоретико-прикладные положения системного анализа аспектов ИЖС, систематизации угроз ИБ, разработанных вариантов их модельного представления позволяют сформулировать системные требования по ИЖС и определить наиболее перспективные пути реализации этих требований в интересах обеспечения радиоэлектронного и информационного превосходства в информационной сфере, живучести ОМТИ в целом на базе приведенных моделей и реализующих их программных комплексов анализа, синтеза и оптимизации ИЖС.

Анализ понятийного аппарата, проблем и технологий реализации ИЖС в свете современных требований и регламентов обеспечения безопасности мореплавания указывает на *особую актуальность* решения сравнительно новой организационно-технической и военно-научной **задачи гарантированного обеспечения информационной живучести корабля, судна** как одного из критических сегментов системы управления безопасностью и живучестью судна.

Литература

1. Бондаренко Д. Л., Жбанов И. Л. Анализ существующих подходов к трактовке понятия «живучесть» информационно-управляющей подсистемы асу специального назначения / Актуальные вопросы технических наук, 2017, с. 100–104.
2. Алексеев А. В. Информационная живучесть судна: понятие, проблемы, технологии / Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 7 / СПОИСУ. – СПб., 2019, с. 345–348.
3. Алексеев А. В. Информационная живучесть управления: теория и практика обеспечения информационного превосходства / Информационная безопасность регионов России (ИБРР-2023). XIII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 25–27 октября 2023 г.: Материалы конференции / СПОИСУ. – СПб, 2023, с. 224–226.
4. Информационные технологии в судостроении: существующие системы, сферы и возможности их использования [Электронный ресурс] URL: https://uchimsya.com/a/qC363Pr9 (дата обращения 24.05.2023).
5. Анфилатов В. С., Емельянов А. А., Кукушкин А. А. Системный анализ в управлении. – М.: Финансы и статистика, 2002.
6. Алексеев А. В., Смольников А. В., Сус Г. Н., Ушакова Н. П. Когнитивные технологии системы поддержки принятия решений и управления борьбой за живучесть корабля, судна // Системы управления и обработки информации: научн.-техн. сб. /АО «Концерн «НПО «Аврора». СПб, 2019. Вып. 3(46), с. 18–27.
7. Алексеев А. В., Кузнецов В. В., Согонов С. А., Мусатенко Р. И., Тычинин И. Ю., Балицкая К. В. Обоснование системы критериев оценки информационной живучести судна / Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 7 / СПОИСУ. – СПб., 2019, с. 353–358.
8. Алексеев А. В., Кузнецов В. В., Согонов С. А., Мусатенко Р. И., Тычинин И. Ю., Балицкая К. В. Система критериев оценки информационной живучести судна / Информационная безопасность регионов России (ИБРР-2019). – СПб., 2019, с. 329-330.
9. Бобрович В. Ю., Алексеев А. В., Антипов В. В., Смольников А. В. Информационная живучесть корабля: угрозы, модель, системные требования, пути реализации / Информационная безопасность регионов России (ИБРР – 2021). – СПб., 2021, с. 265–267.
10. Алексеев А. В. Модель и программный комплекс цифровой трансформации кибербезопасности / Вопросы обеспечения безопасности в киберпространстве: материалы Всероссийской НТК – Махачкала: ДГТУ, 2022 г. – 387 с. с. 251–255.
11. Кибербезопасность в 2023-2024 гг.: тренды и прогнозы. URL: https://ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-v-2023-2024-gg-trendy-i-prognozy-chast-pyataya/ (дата обращения: 25.05.2025).
12. Бондырев В. Е., Дригола В. К., Устинович Е. С., Алексеев А. В. Применение искусственного интеллекта в ВМФ при разработке и принятии управленческих решений / Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 13 / СПОИСУ. – СПб., 2024, 415–420.

INFORMATION SURVIVABILITY OF A SHIP: AN APPLIED THEORY OF ENSURING MILITARY AND TECHNOLOGICAL SUPERIORITY

Alekseev A. V.[4], Drigola V. K.[5], Mikhalchuk A. V.[6]

Keywords: *goal setting; model; ship survivability; monitoring; valid control; vulnerability; threat; confidentiality; accessibility; integrity.*

4 Anatoly V. Alekseev, Dr.Sc. of Technical Sciences, Professor, Professor of the Department of Ship Automation and Measurements, St. Petersburg State Marine Technical University, St. Petersburg, Russia. E-mail: iapbgks@bk.ru

5 Vladimir K. Drigola, Ph.D. of Military Sciences, Senior Researcher of the Military Training and Research Center of the Navy «Naval Academy named after N. G. Kuznetsov», St. Petersburg, Russia. E-mail: velena.spb@mail.ru

6 Andrey V. Mikhalchuk, Ph.D. of Technical Sciences, Associate Professor of the Department of Ship Automation and Measurements, St. Petersburg State Marine Technical University, St. Petersburg, Russia. E-mail: 335mav@mail.ru

Abstract

The purpose of the work *is to substantiate the need to expand the concept of survivability of a ship and to develop the basic principles of the applied theory of information survivability of a ship, vessel (and LC). to ensure military and technological superiority.*

Research method: *systematization of data from the analysis, synthesis and optimization of IHS based on a qualimetric assessment of the aggregated indicator of the design quality and operational efficiency of the integrated information protection system (ICSI) as part of an automated information processing system in a secure design (ASSI).*

The results of the study *include typical structural models of residential housing, the SCSI, a verbal model of residential housing vulnerabilities and threats, a complex mathematical model for assessing and optimizing residential housing, a structural information model of the digital twin of the SCSI and an example of software implementation in the variant of the KASOR-24.4 robotic design complex, and the results of the formation of the applied theory of residential housing.*

The scientific novelty and practical value *of the research consists in the generalization and development of applied theoretical aspects of the introduction and model representation of the analysis, synthesis and optimization of a new concept for the shipbuilding industry, «information survivability of a ship». This made it possible to expand the survivability category of the vessel and for the first time quantify/digitalize such relevant factors of information technology development today as the security of the ship's information resources, their confidentiality, accessibility, integrity, while ensuring military, scientific and technological superiority over a potential adversary.*

References

1. Bondarenko D. L., Zhbanov I. L. Analiz sushhestvujushhih podhodov k traktovke ponjatija «zhivuchest'» informacionno-upravljajushhej podsistemy asu special'nogo naznachenija / Aktual'nye voprosy tehnicheskih nauk, 2017, s. 100–104.
2. Alekseev A. V. Informacionnaja zhivuchest' sudna: ponjatie, problemy, tehnologii / Regional'naja informatika i informacionnaja bezopasnost'. Sbornik trudov. Vypusk 7 / SPOISU. – SPb., 2019, s. 345 – 348.
3. Alekseev A. V. Informacionnaja zhivuchest' upravlenija: teorija i praktika obespechenija informacionnogo prevoshodstva / Informacionnaja bezopasnost' regionov Rossii (IBRR – 2023). XIII Sankt-Peterburgskaja mezhregional'naja konferencija. Sankt-Peterburg, 25–27 oktjabrja 2023 g.: Materialy konferencii / SPOISU. – SPb, 2023, s. 224–226.
4. Informacionnye tehnologii v sudostroenii: sushhestvujushhie sistemy, sfery i vozmozhnosti ih ispol'zovanija [Jelektronnyj resurs] URL: https://uchimsya.com/a/qC363Pr9 (data obrashhenija 24.05.2023).
5. Anfilatov V. S., Emel'janov A. A., Kukushkin A. A. Sistemnyj analiz v upravlenii. – M.: Finansy i statistika, 2002.
6. Alekseev A. V., Smol'nikov A. V., Sus G. N., Ushakova N. P. Kognitivnye tehnologii sistemy podderzhki prinjatija reshenij i upravlenija bor'boj za zhivuchest' korablja, sudna //Sistemy upravlenija i obrabotki informacii: nauchn.-tehn. sb. / AO «Koncern «NPO «Avrora». SPb, 2019. Vyp. 3(46), s. 18–27.
7. Alekseev A. V., Kuznecov V. V., Sogonov S. A., Musatenko R. I., Tychinin I. Ju., Balickaja K. V. Obosnovanie sistemy kriteriev ocenki informacionnoj zhivuchesti sudna / Regional'naja informatika i informacionnaja bezopasnost'. Sbornik trudov. Vypusk 7 / SPOISU. – SPb., 2019, s. 353–358.
8. Alekseev A. V., Kuznecov V. V., Sogonov S. A., Musatenko R. I., Tychinin I. Ju., Balickaja K. V. Sistema kriteriev ocenki informacionnoj zhivuchesti sudna / Informacionnaja bezopasnost' regionov Rossii (IBRR – 2019). – SPb., 2019, s. 329-330.
9. Bobrovich V. Ju., Alekseev A. V., Antipov V. V., Smol'nikov A. V. Informacionnaja zhivuchest' korablja: ugrozy, model', sistemnye trebovanija, puti realizacii / Informacionnaja bezopasnost' regionov Rossii (IBRR – 2021). – SPb., 2021, s. 265–267.
10. Alekseev A. V. Model' i programmnyj kompleks cifrovoj transformacii kiberbezopasnosti / Voprosy obespechenija bezopasnosti v kiberprostranstve: materialy Vserossijskoj NTK – Mahachkala: DGTU, 2022 g. – 387 s. s. 251–255.
11. Kiberbezopasnost' v 2023-2024 gg.: trendy i prognozy. URL: https://ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-v-2023-2024-gg-trendy-i-prognozy-chast-pyataya/ (data obrashhenija: 25.05.2025).
12. Bondyrev V. E., Drigola V. K., Ustinovich E. S., Alekseev A.V. Primenenie iskusstvennogo intellekta v VMF pri razrabotke i prinjatii upravlencheskih reshenij / Regional'naja informatika i informacionnaja bezopasnost'. Sbornik trudov. Vypusk 13 / SPOISU. – SPb., 2024, 415–420.