

RU

## Культура информационной безопасности морского специалиста и условия ее формирования

Жестовский А. Г., Околот Д. Я., Рудинский И. Д.

**Аннотация.** Целью исследования является детализация структуры и содержания одного из специфических компонентов профессиональной информационной культуры личности – культуры информационной безопасности морского специалиста. В статье рассматривается проблематика формирования культуры информационной безопасности морских специалистов; сформулировано определение культуры информационной безопасности морского специалиста, определены ее признаки и структура, приведен и кратко охарактеризован состав ее компонентов. Научная новизна исследования заключается во введении в научный оборот понятия «культура информационной безопасности морского специалиста», определении состава и содержания этой культуры, а также условий к ее формированию. Результатом исследования является выявление условий и выработка рекомендаций по формированию культуры информационной безопасности морского специалиста.

EN

## Marine Specialist's Information Security Culture and Its Formation Conditions

Zhestovskii A. G., Okolot D. Y., Rudinskiy I. D.

**Abstract.** The paper aims to detail the structure and content of one of the specific components of a person's professional information culture - a marine specialist's information security culture. The article considers the problematic of formation of marine specialists' information security culture; formulates the definition of a marine specialist's information security culture, identifies its characteristics and structure, presents and briefly describes the content of its components. The scientific originality of the research lies in the fact that it introduces the notion "marine specialist's information security culture" into scientific circulation, identifies the content of this culture, as well as the conditions of its formation. The results of the study include identification of conditions and development of recommendations on the formation of a marine specialist's information security culture.

### Введение

Современный этап модернизации отечественной системы профессионального образования обусловлен глобальными интеграционными процессами, характеризующимися, среди прочего, возрастанием требований работодателей к способностям работников использовать информацию, в том числе имеющую служебный либо конфиденциальный характер (Жестовский, Михайловский, Околот и др., 2019).

В соответствии с национальным проектом «Цифровая экономика Российской Федерации», утвержденным в 2019 г., применительно к отечественной системе профессиональной подготовки морских специалистов на первый план выходят компетенции выпускника в профессиональном применении потенциала цифровых технологий (О системе управления..., 2019), включая работу с большими и распределенными базами данных, применение инструментов виртуальной и дополненной реальности, использование методов анализа и добычи данных, а также непрерывного обмена информацией со всеми участниками производственного процесса в условиях практически неограниченного широкополосного доступа в Интернет (О системе управления..., 2019).

По этой причине в период становления информационного общества необходимо подготовить человека к быстрому восприятию и обработке больших объемов информации, обучить его современным средствам, методам и технологиям работы. В настоящее время недостаточно уметь самостоятельно осваивать и накапливать информацию – необходимо научиться такой технологии работы с информацией, когда решения подготавливаются и принимаются на основе коллективного знания. Это говорит о том, что человек должен иметь

определенный уровень культуры обращения с информацией. Для отражения этого факта в педагогической науке был введен термин «информационная культура».

Г. В. Алексеев (2017) указывает на то, что дефицит информационной культуры участников международного обмена, коммерсантов и институтов гражданского общества является одной из причин возникновения дисбаланса между требованиями платформ и инструментов современной коммуникации, с одной стороны, и недостаточной информационной культурой пользователей – с другой.

Текущий период развития общества характеризуется кардинальными изменениями в области взаимодействия человека с информацией, все труднее становится ориентироваться в ее потоках. Формирующиеся у современных морских специалистов гибкость мышления, умение *ориентироваться* в огромном потоке информации становятся значимыми ценностями на протяжении всей их профессиональной деятельности. В то же время информация, обрабатываемая в судовых информационных системах, обладает свойствами конфиденциальности, доступности, достаточности, целостности (Жестовский, Рудинский, 2019). Однако процесс работы с информацией создает и новые риски. В частности, возникают опасности развязывания конвенциональных и даже ядерных конфликтов вследствие несанкционированного проникновения в информационные системы военного назначения, создается информационное оружие, все более острыми становятся действия и столкновения в информационном пространстве и т.д.

Морские суда, как и сухопутные объекты, также оказываются объектами нападений в виртуальном пространстве. Их информационные системы подвержены тем же рискам и информационным угрозам, что и системы иных отраслей (Морские суда часто подвергаются кибератакам, 2018). В результате взлома или несанкционированного доступа к системе мониторинга движения судов злоумышленники могут изменять информацию о размерах и местоположении судов, что способно привести к столкновению с другими кораблями. Поскольку судовая информация в настоящее время во все большей степени носит служебный и/или коммерческий характер, попытки несанкционированного доступа к ней становятся более частыми и изощренными, потери от ее утраты или искажения растут. Следовательно, ее защите необходимо уделять все более серьезное внимание, о чем мы писали в предыдущей работе (Жестовский, Михайловский, Околот и др., 2019, с. 94-102) и в других публикациях.

При разработке современных судовых информационных и интегрированных систем, компонентами которых являются компьютерные сети, отдельные базы данных и расчетные задачи с механизмами обработки данных, следует учитывать, что недостаточная информационная защищенность компонентов или возникновение ошибок в работе судовых информационных систем могут привести к тяжелым последствиям, поэтому вопросы информационной безопасности и защиты информации становятся первоочередными. На сегодняшний день в мировом судоходстве защита информации, хранимой и обрабатываемой в судовых информационных системах, становится такой же актуальной задачей, как обеспечение безопасности и охраны самих судов (Информационная безопасность судов..., 2020).

Поскольку одной из задач безопасного мореплавания является подготовка соответствующих специалистов (Скорыходов, Борисова, Борисов, 2010), специалист-мореплавец должен обладать культурой информационной безопасности, так как даже самая сложная и включающая дополнительные функции судовая система информационной безопасности (СИБ) не обеспечит эффективную защиту информации, если члены судовой команды не будут обладать основами этой культуры, являющейся, по сути, базисом и источником осознанного и ответственного отношения к информации как таковой и к субъектам, которые с ней взаимодействуют.

Культура информационной безопасности, как одна из составляющих социальной безопасности, является одним из приоритетных направлений государственной политики в сфере национальной безопасности России (Концепция общественной безопасности..., 2013). Формирование основ культуры информационной безопасности у граждан рекомендуется в Доктрине информационной безопасности Российской Федерации, где указано «обеспечение защищенности граждан от информационных угроз, в том числе за счет формирования культуры личной информационной безопасности» (Доктрина информационной безопасности..., 2016).

В то же время формирование дополнительных компетенций в сфере информационной безопасности как неотъемлемого компонента культуры информационной безопасности может стать перспективным путем к повышению безопасности личности. Мы разделяем мнение В. А. Девисилова (2008) о том, что «культура как совокупность материальных и духовных ценностей, жизненных представлений, образцов поведения, норм, способов и приемов человеческой деятельности должна включать в себя культуру безопасности» (с. 27-31).

А. А. Дронов, Т. А. Дронова (2015, с. 722) ввели понятие «культура безопасности профессиональной деятельности», под которым они понимают такой комплекс специфических свойств личности специалиста в определенной профессиональной области, который гарантирует достижение необходимого уровня безопасности при осуществлении профессиональной деятельности. В настоящей статье мы рассматриваем культуру информационной безопасности морских специалистов как аспект осуществления ими профессиональной деятельности.

Актуальность принципиально нового подхода к защите судовой информации и формирования профессиональной компетентности морского специалиста обусловлена необходимостью обеспечения этой защиты не только и не столько с помощью современных программно-технических и иных средств, но в первую очередь путем становления у членов экипажа элементов специфической информационной культуры, названной нами культурой информационной безопасности морского специалиста (КИБ МС).

Предметом внимания при формировании КИБ МС являются, по сути, те же содержательные и нормативно-правовые категории, предопределяющие построение и функционирование систем защиты информации на государственном уровне, на уровне предприятия и организации либо на уровне отдельной личности (Ярочкин, 2018). Однако при рассмотрении проблематики КИБ МС на первый план выходят вопросы общекультурного, морально-этического, социально-рефлексивного характера, отражающие культурологическую основу рассматриваемой проблематики. Статистика инцидентов в сфере информационной безопасности свидетельствует, что удельный вес гуманитарных проблем (регулирование отношений и противодействие злоупотреблениям свободой слова в Интернете; правовое регулирование отношений в области противодействия преступлениям в сфере информационно-коммуникационных технологий, формирование системы международной информационной безопасности и т.п.) достигает 80% (Малюк, Алексеева, 2016, с. 46).

Наши выводы об актуальности и необходимости систематического исследования проблематики КИБ МС подтверждает публикация (Астахова, Лушникова, 2019), в которой отмечается недостаточное развитие культуры информационной безопасности в России. В отличие от развитых зарубежных стран, культура информационной безопасности в России рассматривается исключительно как комплекс знаний без конкретизации целевых установок, ценностных ориентиров, нормирования поведения и установления ответственности за несоблюдение принятых правил. Такой подход приводит к усилению угроз, исходящих от пользователей корпоративных информационных систем, и ослабляет внешний периметр их информационной безопасности. Подтверждением недостаточной научно-методической проработанности проблематики формирования КИБ в целом и культуры кибербезопасности личности в частности может служить крайне незначительное количество публикаций по этой тематике. Также отметим, что термин «культура информационной безопасности» почти не знаком научной общественности и в широкой практике почти не применяется.

Среди факторов, ведущих к ослаблению и размыванию культуры информационной безопасности, следует отметить непрерывное возникновение новых рисков, обусловленных стремительной цифровизацией экономики и недостаточной квалификацией специалистов, призванных обеспечивать информационную безопасность предприятия, многочисленными уязвимостями прикладного и системного программного обеспечения, использованием в корыстных целях методов социальной инженерии, недостаточно эффективным противодействием киберпреступности со стороны органов охраны правопорядка (Головки, 2019).

Вопреки расхожему мнению о том, что предотвратить дистанционные кибератаки могут лишь продвинутые антивирусные программы, человеческий фактор остается самым слабым звеном в информационной системе морского судна, тогда как защищенность и устойчивость этой системы обусловлена в первую очередь высоким уровнем осведомленности и ответственности экипажей (Кибербезопасность судна..., 2017, с. 30).

По нашему мнению, недостаточное знание членами судового экипажа основных принципов защиты информации, непонимание либо недопонимание необходимости тщательного выполнения правил и инструкций в сфере информационной безопасности, неаккуратность либо небрежность при работе с судовой информацией могут и должны рассматриваться как признаки отсутствия либо недостаточной сформированности у морского специалиста основ профессиональной культуры информационной безопасности.

Таким образом, формирование культуры информационной безопасности морских специалистов является актуальной и необходимой задачей, решение которой обретает особое значение на фоне стремительного проникновения информационных и коммуникационных технологий во все сферы жизнедеятельности общества.

Задачами исследования являются:

- раскрыть сущность и содержание понятия «культура информационной безопасности морского специалиста»;
- описать условия по формированию культуры информационной безопасности морского специалиста в рамках изучения профессиональных дисциплин.

Теоретическая база. При раскрытии основной проблемы работы мы опирались на труды В. П. Полякова (2012), А. А. Дронова, Т. А. Дроновой (2015), А. А. Малюка, И. Ю. Алексеевой (2016), Е. Н. Боярова (2012), В. С. Горюнова (2016), Н. И. Гендиной, Н. И. Колковой, Г. А. Стародубовой, Ю. В. Уленко (2006), Л. В. Астаховой, С. С. Лушниковой (2019). Указанные труды перечисленных ученых посвящены формированию информационной культуры личности и культуры информационной безопасности специалистов, а также формированию культуры безопасности в профессиональной деятельности.

При этом необходимо отметить, что данные исследователи не затрагивают проблему, указанную в теме статьи, их исследования, по большей части, затрагивают похожее понятие «культура информационной безопасности». Мы же рассматриваем более узкий слой носителей такой культуры – морских специалистов, а также особенности осуществления ими профессиональной деятельности, связанной с мореплаванием и обеспечением его безопасности.

Проведенный нами анализ как отечественных, так и зарубежных источников свидетельствует об отсутствии в работах научного обоснования понятия «культура информационной безопасности морского специалиста». По нашему мнению, введение этого понятия в специализированный оборот позволит привлечь внимание специалистов к рассматриваемой проблеме и выработать необходимые профессиональные решения.

Методы исследования. Теоретический этап исследования предполагал анализ отечественной педагогической литературы и практики. Для подтверждения эффективности результатов статьи применены методы декомпозиции и предложены варианты, в рамках каких дисциплин может формироваться культура информационной безопасности морского специалиста.

Практическая значимость. В практическом плане работа может быть также использована при разработке рекомендаций и концептуальных подходов в области обеспечения информационной безопасности судна. Результаты исследования внедрены в образовательный процесс Балтийской государственной академии рыбопромыслового флота ФГБОУ ВО «КГТУ» и могут быть использованы в других учебных заведениях.

### **Сущность и содержание понятия «культура информационной безопасности морского специалиста»**

В настоящей работе под культурой информационной безопасности морского специалиста мы будем понимать «систему знаний, умений и навыков в области обеспечения информационной безопасности судовых информационных систем, гарантирующую их последующее применение носителем этой культуры для достижения необходимого и достаточного уровня информационной безопасности судовой информационной системы» (Рудинский, Околот, 2019, с. 30).

Важнейшим компонентом культуры информационной безопасности морского специалиста становятся умение, способность и готовность защитить информацию в судовой информационной системе от реальных или вероятных угроз и обеспечить ее безопасность (Бояров, 2012).

Как отмечалось в другой работе авторов (Рудинский, Околот, 2019, с. 33), формирование культуры информационной безопасности морских специалистов должно базироваться на основах, закладываемых с самых первых этапов семейного воспитания, с ее последующим закреплением и развитием на всех уровнях как общего, так и профессионального образования. В первую очередь речь идет о базовых навыках информационной безопасности, например, не раскрывать «семейные тайны» друзьям и знакомым, не разговаривать с незнакомыми людьми, не предоставлять посторонним доступ к своему персональному телефону и т.п.

Культура информационной безопасности является частью общей культуры как интегрального качества любой личности вне зависимости от профессии, уровня образования, ценностных и иных ориентиров человека, поскольку каждый человек обладает определёнными жизненными принципами, культурой поведения, этикетом, манерами и т.п. (Гендина, Колкова, Стародубова и др., 2006). Соответственно, КИБ МС, с одной стороны, выступает несомненным компонентом общей культуры как умение грамотно получать и обрабатывать информацию, а также управлять процессом ее распространения. С другой стороны, КИБ МС является специфическим свойством конкретной категории морских специалистов (КИБ МС необходима только для них, поскольку обеспечение безопасности судовых информационных систем является одним из видов их профессиональной деятельности).

По нашему мнению, в качестве базовых признаков культуры информационной безопасности морского специалиста выступают:

- способность морского специалиста получать из различных источников информацию, полезную и/или необходимую для достижения целей судовой информационной системы;
- способность морского специалиста анализировать и сортировать полученную информацию по критериям достоверности, полезности и безопасности;
- осознание морским специалистом возможности распространения (в том числе публикации) только той судовой информации, которая не наносит ущерб себе, другим членам экипажа, мореходной компании и обществу в целом.

С учетом перечисленных признаков мы рассматриваем КИБ МС как специализированный компонент общей информационной культуры личности в ее социотехническом и информационно-технологическом аспекте и, одновременно, как компонент профессиональной культуры личности (Горюнов, 2016, с. 337).

Сформулированное нами определение КИБ МС отличается от определения, приведенного в прошлой работе авторов (Рудинский, Околот, 2019, с. 30) конкретизацией прикладной сферы применения компетенций в области информационной безопасности, то есть морской спецификой. Поэтому целенаправленное и систематическое формирование такой культуры возможно только на базе соответствующих организаций профессионального образования, осуществляющих подготовку морских специалистов.

Мы также разделяем мнение В. П. Полякова (2012, с. 4) о том, что «подготовка в области информационной безопасности и защиты информации на этапе общего образования нуждается в совершенствовании и развитии, а профессиональные знания в этой области обязательно должны быть дополнены на следующих ступенях образования».

По нашему мнению, формирование культуры информационной безопасности морских специалистов должно осуществляться на базе системно-деятельностного (Пургина, 2015) и компетентностного (Рудинский, Давыдова, Петров, 2019) подходов.

Под системно-деятельностным подходом понимается такой способ организации учебно-познавательной деятельности обучающихся, при котором они являются не пассивными «приемниками» информации, а сами активно участвуют в учебном процессе (Котова, 2016).

В частности, применение системно-деятельностного подхода для формирования культуры информационной безопасности морских специалистов позволяет сформировать систему знаний и установок, необходимых для организации информационной безопасности судна. Указанный подход позволяет:

- сформировать у обучающихся мотивационные и познавательные установки (желание узнать и научиться применять технологии, методы и приемы обеспечения безопасности судовых информационных систем),

а также конкретную учебную цель (понимание, что именно необходимо выяснить и освоить для достижения и поддержания должного уровня безопасности конкретной судовой информационной системы);

- обеспечить самостоятельное выполнение обучающимися определённых действий для получения недостающих знаний в процессе учебного исследования под руководством преподавателя, в том числе изучение тематической литературы и технической документации, консультации с опытными специалистами в области информационной безопасности и т.п.

Компетентностный подход представляет собой способ организации образовательного процесса, направленный на формирование компетентности индивида в конкретной профессиональной области профессиональной деятельности (Рудинский, Давыдова, Петров, 2019).

Компетентностный подход к формированию КИБ МС усиливает практическую направленность процесса обучения, подчеркивает необходимость обретения обучающимися умений и опыта получать новые знания и применять их на практике. По этой причине формирование профессиональной компетентности в области обеспечения информационной безопасности судовых информационных систем и культуры в информационной безопасности в этой отрасли не завершается приобретением квалификации специалиста, развитие профессиональной компетентности продолжается на протяжении всей профессиональной деятельности (Околот, Рудинский, 2020).

При этом далеко не завершённые исследования состава, структуры и содержания культуры информационной безопасности морских специалистов позволяют характеризовать ее как обязательный элемент профессиональной информационной культуры морского специалиста, определяющий его способность и готовность обеспечить защиту судовой информации и решений по безопасному управлению судном. С позиций морского специалиста как носителя этой культуры КИБ МС представляется специфическим свойством индивида, которое может быть системно структурировано взаимосвязями когнитивного, функционального, мотивационного, личностного компонентов этой культуры (Рисунок 1). Приведем краткую характеристику каждого компонента.



**Рисунок 1.** Структура и содержание культуры информационной безопасности морского специалиста

Когнитивный компонент КИБ МС отражает знания морского специалиста об основных понятиях и задачах, административно-процедурных мерах и регламентах обеспечения информационной безопасности судовых информационных систем как в сфере профессиональной деятельности, так и в индивидуальном информационном пространстве. Основу этого компонента составляют знания об основных угрозах и уязвимостях информации в судовых информационных системах, мерах по их устранению, основных каналах утечки конфиденциальной судовой информации и способах ее защиты.

Функциональный компонент КИБ МС характеризуется профессиональными действиями по выработке и реализации комплекса мер для обеспечения информационной безопасности судовых информационных систем. Функциональный компонент также предполагает способность морского специалиста составлять и анализировать модели угроз и нарушений информационной безопасности с целью их предотвращения,

а также проводить мониторинг защищенности судовой информационной системы. Еще один важнейший элемент КИБ МС – умение применять нормативные правовые акты и методические документы в области обеспечения защиты судовой конфиденциальной информации.

*Мотивационный* компонент КИБ МС включает в себя систему причин, мотивов и оснований для реализации морским специалистом конкретных процедур и регламентов обработки судовой информации, включая определение возможности предоставления доступа к ней третьих лиц.

*Личностный* компонент КБ МС включает в себя персональные качества морского специалиста, характеризующие его готовность и возможность исполнять обязанности по защите судовой информации, а также предопределяющие успешность и результативность этой деятельности.

По нашему мнению, именно так представляется состав культуры информационной безопасности морского специалиста. На основании изложенного можно сделать вывод о том, что культура информационной безопасности морского специалиста – это часть базовой культуры, интегральное качество личности морского специалиста, включающее в себя когнитивный, функциональный, мотивационный и личностный компоненты. Эти компоненты отражают готовность морского специалиста к безопасному осуществлению профессиональной деятельности, а также способность обеспечить информационную безопасность судна.

### **Условия формирования культуры информационной безопасности морского специалиста в рамках изучения профессиональных дисциплин**

Формирование указанных выше компонентов КИБ МС (когнитивного, функционального, мотивационного, личностного) как части профессиональной компетентности морского специалиста должно осуществляться в процессе получения им профессионального образования.

С позиций компетентностного подхода (Рудинский, Давыдова, Петров, 2019) важнейшим условием достижения требуемого уровня культуры информационной безопасности морского специалиста является формирование у него общепрофессиональной компетенции в области защиты судовой информации, состоящей в способности и готовности обеспечить защиту судовой информации и решений по безопасному управлению судном (Жестовский, Михайловский, Околот и др., 2019). Результативность формирования у морских специалистов указанной компетенции будет определяться как реализацией циклов дисциплин классического академического характера, так и специфической профессиональной подготовкой непосредственно в морских условиях.

В частности, в процессе изучения универсальной дисциплины «Информатика» должно предусматриваться формирование таких составляющих когнитивного и функционального компонентов КИБ МС, как знание и умение применять нормативные правовые акты и методические документы в области защиты судовой конфиденциальной информации, общая информационная культура студентов и подготовка студентов к использованию современных информационных технологий как в сфере будущей профессиональной деятельности, так и в индивидуальном информационном пространстве в контексте обеспечения их собственной безопасности, активно используя интерактивные методы обучения, предусматривающие совместное обучение студента и преподавателя.

При изучении дисциплины «Безопасность жизнедеятельности» должен формироваться мотивационный компонент КИБ МС, связанный с осознанной необходимостью обеспечивать и поддерживать информационную безопасность морского судна. Используются такие дидактические приемы, как выделение главного, существенного в изученном материале; установление аналогии, систематизация, сравнение и др., мотивируя обучающегося на получение базовых сведений по защите судовой конфиденциальной информации и создавая представление студентов об информационных угрозах системе управления судном. Эти приемы позволяют развивать способность к логическому рассуждению и к осознанию самого себя в мире киберпространства.

В рамках изучения дисциплины «Основы информационной безопасности» у будущих морских специалистов должен быть сформирован личностный компонент КИБ, определяющий их готовность обеспечивать безопасность и целостность информационной системы морского судна.

Отдельные элементы культуры информационной безопасности будущего морского специалиста могут дополнительно формироваться и развиваться в рамках изучения таких профильных дисциплин общепрофессионального модуля, как «Интеллектуальные системы поддержки принятия решений в сложных ситуациях» и «Информационные технологии управления», а также факультативной дисциплины «Основы защиты информации в судовых информационных системах».

Условия и цели изложения учебного материала по указанным дисциплинам были определены исходя из необходимости формирования обсуждаемой культуры информационной безопасности морского специалиста. Так, основной целью освоения темы «Программно-аппаратные средства защиты судовой информации» для дисциплины «Основы защиты информации в судовых информационных системах» является получение общих сведений о формах и методах защиты судовой информации штатными средствами, а также приобретение практических навыков по организации парольной и криптографической защиты информации, разграничению прав доступа для различных пользователей и штатному восстановлению работоспособности системы после сбоя.

В рамках профильной дисциплины «Интеллектуальные системы поддержки принятия решений в сложных ситуациях» признано целесообразным изучение темы «Основы информационной безопасности судовой информационной системы», в процессе рассмотрения которой обучающиеся смогут узнать об основных рисках и угрозах судну и судовым информационным системам, а также о способах их нейтрализации и сведения к минимуму.

В тематический план дисциплины «Безопасность жизнедеятельности» предлагается ввести тему «Основы безопасности мореплавания», в ходе изучения которой обучающиеся смогут узнать о проблемах организации безопасности судоходства и методах обеспечения безопасности мореплавания.

Таким образом, в ходе изучения указанных дисциплин могут быть сформированы основы КИБ МС. Морской специалист, который овладел культурой информационной безопасности, более склонен не только к охране своей жизни и здоровья, но и к безопасному осуществлению профессиональной деятельности. В качестве условий формирования КИБ МС также можно указать: наличие безопасной информационной образовательной среды как образовательного пространства эффективного формирования КИБ МС; реализацию культуроориентированных образовательных технологий как одного из системных факторов образовательного процесса; ориентацию целей изучения дисциплин универсального и общепрофессионального характера на формирование основ КИБ МС; разработку и систематическое применение специализированного диагностического инструментария для определения уровней сформированности КИБ МС.

## Заключение

Подготовка будущих специалистов, обладающих должным уровнем культуры информационной безопасности и соответствующих все более серьезным требованиям информационного общества, является одним из приоритетных направлений современного профессионального образования.

Деятельность по формированию культуры информационной безопасности морского специалиста – это длительный процесс, охватывающий не только период его подготовки в морском вузе, но и практически весь период профессиональной деятельности. Поскольку в подавляющем большинстве случаев реализации угроз информационной безопасности морских судов определяющим является человеческий фактор, для предотвращения этих угроз у каждого члена экипажа должна быть сформирована культура информационной безопасности.

Предпринятая нами попытка сформулировать понятие «культура информационной безопасности морского специалиста», определить ее место, роль и значение как элемента информационной и общей культуры этого специалиста, а также структурировать компонентный состав исследуемого феномена позволяет заложить основы разработки и комплексной реализации системы мероприятий, основанных на инновационных подходах к обеспечению защищенности информации, циркулирующей в судовой информационной системе.

Формирование культуры информационной безопасности морского специалиста должно осуществляться при изучении профессиональных дисциплин при использовании таких подходов, как системно-деятельностный и компетентностный, которые позволяют сформировать у обучающихся необходимые мотивационные и познавательные установки и усилить практическую направленность образовательного процесса.

Перспективы дальнейшего исследования будут связаны с проведением исследования по формированию культуры информационной безопасности у других специалистов похожих направлений профессиональной деятельности.

## Источники | References

1. Алексеев Г. В. Расширение областей применения информационных технологий и информационная безопасность государства // *Управленческое консультирование*. 2017. № 5 (101).
2. Астахова Л. В., Лушникова С. С. Культура информационной безопасности предприятия: сравнительный анализ зарубежных и российских исследований // *Вестник УрФО. Безопасность в информационной сфере*. 2019. № 1 (31).
3. Бояров Е. Н. Информационная культура современного специалиста образования в области безопасности жизнедеятельности // *Безопасность жизнедеятельности: наука, образование, практика: материалы II международной научно-практической конференции* (г. Южно-Сахалинск, 28 ноября 2011 г.): сборник научных статей / сост. С. В. Абрамова, В. В. Моисеев, Е. Н. Бояров. Южно-Сахалинск: Изд-во СахГУ, 2012.
4. Гендина Н. И., Колкова Н. И., Стародубова Г. А. и др. Формирование информационной культуры личности: теоретическое обоснование и моделирование содержания учебной дисциплины. М.: Межрегиональный центр библиотечного сотрудничества, 2006.
5. Головкин Н. Прогноз развития киберугроз и средств защиты информации 2020. 2019. URL: [https://www.anti-malware.ru/analytics/Threats\\_Analysis/cyber-threats-and-security-tools-evolving-2020-forecast](https://www.anti-malware.ru/analytics/Threats_Analysis/cyber-threats-and-security-tools-evolving-2020-forecast)
6. Горюнов В. С. Информационная культура как необходимая часть развития современного человека в условиях формирующегося глобального информационного общества. 2016. URL: <https://e-koncept.ru/2016/86969.htm>
7. Девисилов В. А. Концептуальные основы образования в области безопасности // *Высшее образование в России*. 2008. № 9.
8. Доктрина информационной безопасности Российской Федерации: указ Президента Российской Федерации от 05 декабря 2016 г. № 646. 2016. URL: <https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html>
9. Дронов А. А., Дронова Т. А. Культура безопасности в профессиональной деятельности // *Акмеология: научно-практический журнал*. 2015. № 3 (55).

10. Жестовский А. Г., Михайловский М. Ю., Околот Д. Я. и др. Проблемы информационной безопасности судовой информационной системы и пути их решения при подготовке специалистов мореходных направлений // Морские интеллектуальные технологии. 2019. Т. 4. № 4 (46).
11. Жестовский А. Г., Рудинский И. Д. Принципы и способы подготовки морских специалистов в области защиты судовой информации // Материалы VII Международного Балтийского морского форума (г. Калининград, 07-12 октября 2019 г.). Калининград, 2019.
12. Информационная безопасность судов (Кибербезопасность). 2020. URL: <https://ibicon.ru/cyber-security>
13. Кибербезопасность судна - в руках моряков // Морской профсоюзный вестник. 2017. № 6 (117).
14. Концепция общественной безопасности в Российской Федерации: утверждена Президентом Российской Федерации 14.11.2013 № Пр-2685. 2013. URL: <http://www.kremlin.ru/acts/news/19653>
15. Котова С. К. Системно-деятельностный подход в реализации ФГОС НОО. 2016. URL: <http://e-koncept.ru/2016/56247.htm>
16. Малюк А. А., Алексеева И. Ю. Культура информационной безопасности как элемент подготовки специалистов по защите информации // История и архивы. 2016. № 1 (3).
17. Морские суда часто подвергаются кибератакам. 2018. URL: <https://www.securitylab.ru/news/497004.php>
18. О системе управления реализацией национальной программы «Цифровая экономика Российской Федерации»: распоряжение Правительства Российской Федерации от 2 марта 2019 г. № 234. 2019. URL: <http://pravo.gov.ru/proxy/ips/?docbody=&prevDoc=102636081&backlink=1&&nd=102525856>
19. Околот Д. Я., Рудинский И. Д. Компетентностный подход в подготовке специалистов в области информационной безопасности в учреждениях среднего профессионального образования. 2020. URL: <https://koirojournal.ru/realises/g2020/3jul2020/kvo205/>
20. Поляков В. П. О непрерывности образования в области информационной безопасности // Известия Российской академии образования. 2012. № 2.
21. Пургина Е. И. Методологические подходы в современном образовании и педагогической науке: учебное пособие. Екатеринбург, 2015.
22. Рудинский И. Д., Давыдова Н. А., Петров С. В. Компетенция. Компетентность. Компетентностный подход. Изд-е 2-е, испр. / под ред. И. Д. Рудинского. М.: Горячая линия - Телеком, 2019.
23. Рудинский И. Д., Околот Д. Я. Формирование культуры информационной безопасности студентов колледжа // Информатика и образование. 2019. № 9.
24. Скороходов Д. А., Борисова Л. Ф., Борисов З. Д. Принципы и категории обеспечения безопасности мореплавания // Вестник Мурманского государственного технического университета. 2010. Т. 13. № 4/1.
25. Ярочкин В. И. Информационная безопасность: учебник для вузов. М.: Академический Проект, 2018.

### Информация об авторах | Author information

**RU****Жестовский Александр Георгиевич<sup>1</sup>****Околот Денис Ярославович<sup>2</sup>****Рудинский Игорь Давидович<sup>3</sup>**, д. пед. н., проф.<sup>1</sup> Балтийская государственная академия рыбопромыслового флота, г. Калининград;

Калининградский государственный технический университет

<sup>2</sup> Балтийский информационный техникум, г. Калининград<sup>3</sup> Балтийский федеральный университет им. И. Канта, г. Калининград**EN****Zhestovskii Aleksandr Georgievich<sup>1</sup>****Okolot Denis Yaroslavovich<sup>2</sup>****Rudinskiy Igor Davidovich<sup>3</sup>**, Dr<sup>1</sup> Baltic Fishing Fleet State Academy, Kaliningrad;

Kaliningrad State Technical University

<sup>2</sup> Baltic Information Technical College<sup>3</sup> Immanuel Kant Baltic Federal University, Kaliningrad<sup>1</sup> [a.zhestovskiy@bk.ru](mailto:a.zhestovskiy@bk.ru), <sup>2</sup> [d.y.okolot@yandex.ru](mailto:d.y.okolot@yandex.ru), <sup>3</sup> [irudinskii@kantiana.ru](mailto:irudinskii@kantiana.ru)

### Информация о статье | About this article

Дата поступления рукописи (received): 13.12.2021; опубликовано (published): 28.02.2022.

**Ключевые слова (keywords):** культура информационной безопасности; структура; компоненты; подготовка морских специалистов; профессиональное образование; information security culture; structure; components; marine specialists training; vocational education.