Вестник Череповецкого государственного университета. 2023. № 3 (114). С. 249–260.
Cherepovets State University Bulletin, 2023, no. 3 (114), pp. 249–260.

Научная статья
УДК 378.1
https://doi.org/10.23859/1994-0637-2023-3-114-20

Профессиональные компетенции бакалавров по информационной безопасности

Татьяна Ароновна Лавина[1]✉, Лариса Алексеевна Ильина[2], Дмитрий Владимирович Ильин[3]
[1, 2, 3] Чувашский государственный университет им. И. Н. Ульянова, Чебоксары, Россия
[1]✉tlavina@mail.ru, https://orcid.org/0000-0002-1825-0097
[2]larisai2009@gmail.com, https://orcid.org/0000-0001-8550-2429
[3]destr@mail.ru, https://orcid.org/0000-0003-2179-7429

Аннотация. В статье рассматривается определение профессиональных компетенций бакалавров по информационной безопасности. Исследования, посвященные подготовке кадров, обеспечивающих защиту информации, соблюдение требований международных и профессиональных стандартов, и анализ запросов профессионального сообщества к кандидатам на должности позволили определить профессиональные компетенции и составляющие их компоненты. Для сравнительного анализа используются разработанные вузами профессиональные компетенции для программ подготовки бакалавров, представленные на официальных сайтах организаций.

Ключевые слова: профессиональные компетенции, профессиональные стандарты в области информационной безопасности, квалификационные характеристики, запросы работодателей
Для цитирования: *Лавина Т. А., Ильина Л. А., Ильин Д. В.* Профессиональные компетенции бакалавров по информационной безопасности // Вестник Череповецкого государственного университета. 2023. № 3 (114). С. 249–260. https://doi.org/10.23859/1994-0637-2023-3-114-20.

Bachelors' professional competencies in information security

Tatyana A. Lavina[1]✉*, Larisa A. Ilina[2], Dmitry V. Ilyn[3]
[1, 2, 3] I. N. Ulianov Chuvash State University, Cheboksary, Russia
tlavina@mail.ru✉, https://orcid.org/0000-0002-1825-0097
larisai2009@gmail.com, https://orcid.org/0000-0001-8550-2429
destr@mail.ru, https://orcid.org/0000-0003-2179-7429

Abstract. The article discusses the definition of bachelors' professional competencies in information security. Research on information security training of personnel ensuring the protection of information, compliance with international and professional standards and analysis of professional community requests for job candidates allowed defining professional competencies and their

components. For comparative analysis, the authors used professional competences developed by universities for bachelor training programmes, presented on the official websites of the organisations.
Keywords: professional competencies, professional standards in the field of information security, qualification characteristics, employers' requests
For citation: Lavina T. A., Ilina L. A., Ilyn D. V. Bachelors' professional competencies in information security. *Cherepovets State University Bulletin*, 2023, no. 3 (114), pp. 249–260. https://doi.org/10.23859/1994-0637-2023-3-114-20.

Введение

Информационная безопасность (ИБ) является ключевым аспектом государственной политики. Стремительное развитие информационных и коммуникационных технологий (ИКТ) приводит к росту информационных угроз как для общества, так и для государства. Все государства имеют собственные стандарты в этой сфере. Разработано и международное законодательство, регулирующее данные вопросы. В Российской Федерации (РФ) действует Доктрина ИБ[1], которая отражает официальные взгляды на обеспечение национальной безопасности нашего государства в сфере информационных технологий (ИТ). Кроме того, президентом РФ в 2021 году утверждена «Стратегия национальной безопасности РФ» (Стратегия). В этом документе рассматриваются вопросы, касающиеся обеспечения ИБ при решении задач, связанных с формированием безопасной информационной инфраструктуры, а также с ее устойчивым функционированием. Не менее важно развивать систему прогнозирования, выявления и предупреждения угроз ИБ РФ, способствовать скорейшей ликвидации последствий, в случае осуществления этих угроз. Необходимым аспектом в организации системы ИБ становится подготовка кадров, обеспечивающих защиту информации (ЗИ). Требования к компетенциям специалистов по ИБ представлены и в международных стандартах ISO/IEC 27021:2017 [2].

В связи с растущими внутренними и внешними информационными угрозами постоянно возрастают и требования к квалификации работников в сфере ИБ, о чем свидетельствуют изменения, внесенные в профессиональные стандарты (ПС) в 2022 году.

Исследования М. С. Анурьевой[3], Е. В. Бурьковой[4], А. А. Кравцова[1], Е. А. Помельниковой[2], посвященные подготовке к успешной профессиональной деятельно-

[1] Доктрина информационной безопасности Российской Федерации. URL: http://base.garant.ru/71556224 (дата обращения: 15.01.2023).

[2] ISO/IEC 27021:2017 "Information technology – Security techniques – Competence requirements for information security management systems professionals", IDT.

[3] Анурьева М. С. Направления развития отечественной системы подготовки специалистов по защите информации // Вестник Тамбовского университета. Серия: Естественные и технические науки. 2013. Т. 18. Вып. 1. С. 230–232.

[4] Бурькова Е. В. Профессиональная подготовка специалистов в области информационной безопасности // Вестник Оренбургского государственного университета. 2016. № 2 (190). С. 3–9.

сти специалистов по ИБ, свидетельствуют о том, что повышение качества образования в этой сфере является актуальной проблемой.

Подготовка кадров в системе высшего образования (ВО) осуществляется по Федеральным государственным образовательным стандартам (ФГОС), формирующим компетенции, при помощи которых оцениваются образовательные результаты. Имеется большое количество работ по компетентностному подходу (В. И. Байденко, И. А. Зимняя, Э. Ф. Зеер, А. В. Хуторской др.). В связи с отсутствием общего подхода к определению компентенции, под данным понятием мы будем подразумевать готовность выпускника применить полученные знания и опыт в области ИБ[3].

Имеются исследования, посвященные определению профессиональных компетенций (ПК) по направлениям подготовки в области ИТ[4], но не в сфере ИБ и по компонентам ПК[5]. Профессиональные компетенции выявляют способности выпускника к работе в конкретных областях в соответствии с направлением подготовки и профилем образовательной программы (ОП). Согласно требованиям действующих ФГОС ВО компетенции формулируются самостоятельно образовательными организациями (ОО). Наряду с определением содержания ОО к каждой из ПК также необходимо разработать индикаторы, которые позволят оценить итоговое освоение компетенции. Эта деятельность осуществляется на основе требований ПС, с учетом запросов работодателей (перспектив развития рынка).

В Чувашском государственном университете имени И. Н. Ульянова обучение бакалавров по ИБ реализуется по профилю «Информационно-аналитические системы финансового мониторинга». При составлении ОП в разделе, затрагивающем ПК (содержание, индикаторы, перечень дисциплин и практик в учебном плане), учитывались требования ПС в области ИБ, а также требования профессионального сообщества. ОП согласованы с работодателями, в них включены дисциплины, рекомендованные организациями-партнерами в части, создаваемой участниками образовательных отношений. Данные дисциплины направлены на формирование ПК.

Основная часть

Попытки сформулировать общий подход к компетенциям в области ИБ предпринимаются достаточно давно. Н. Г. Милославская и А. И. Толстой в исследовании о

[1] Кравцов А. А. Специфика профессиональной подготовки студентов по направлению «Информационная безопасность» // Вестник Московского государственного лингвистического университета. 2013. № 16 (676). С. 137–149.

[2] Помельникова Е. А. Формирование готовности будущих специалистов по ИБ к успешной профессиональной деятельности: дис. … канд. пед. наук. Самара: [б. и.], 2019. 183 с.

[3] Лавина Т. А., Ильина Л. А. ИКТ-компетентность будущих специалистов по защите информации // Вестник Череповецкого государственного университета. 2021. № 6 (105). С. 112–128.

[4] Лавина Т. А., Мытникова Е. А., Давыдова О. В. Профессиональные компетенции бакалавров по направлению «Программная инженерия» // Вестник Череповецкого государственного университета. 2022. № 5 (110). С. 218–226.

[5] Кобзева Н. И. Профессиональные компетенции в контексте компетентностно-ориентированного подхода в образовании // Вестник Оренбургского государственного университета. 2018. № 5 (217). С. 36–42.

компетентностных требованиях стандартов ISO/IEC к профессионалам в области ИБ[1] первые попытки сделать это относят к концу 1990-х гг., в связи с началом проведения конференций, направленных на обучение ИБ. Авторы выделяют три базовых международных подхода: американский, разработанный на основе нормативных документов Департамента национальной безопасности США[2]; австралийский, составленный офисом информационного менеджмента правительства Австралии[3], и европейский, основанный на Европейской модели электронной компетентности e-CF 3.0[4].

В новом Национальном стандарте РФ[5] (введен в действие с 30.11.2021), основанном на международных стандартах по ИБ ISO[2], представлены компетентностные требования к специалистам по системам менеджмента ИБ. Эти стандарты предназначены в том числе и для образовательных учреждений для согласования ОП в области ИБ.

В исследовании Д. С. Васильевой и А. В. Шабуровой[6] в структуре компетенций специалиста по ИБ выделяются: техническая безопасность, управление ИБ, расследование угроз и защита от их возникновения.

Для того, чтобы определить содержание ПК бакалавров по ИБ, в соответствии с требованиями ФГОС ВО, рассмотрим требования к квалификации бакалавров по ИБ из реестра ПС, а также основные запросы рынка труда.

Сначала проведем выборку общепрофессиональных компетенций (ОПК) из ФГОС ВО по направлению 10.03.01 «Информационная безопасность»[7], связанных с осуществлением трудовых функций (ТФ) в области ИБ, для исключения их дублирования при определении ПК. Это компетенции ОПК-1, 5, 6, 10, 12, формирующие следующие способности: оценивать роль информации, ИТ и ИБ, их значимость в обеспечении объективных потребностей личности, общества и государства; приме-

[1] Милославская Н. Г., Толстой А. И. Компетентностные требования стандартов ISO/IEC к профессионалам в области информационной безопасности // Безопасность информационных систем. 2017. Т. 24. № 4. С. 6–18.

[2] State Government Information Security Workforce Development Model. A Best Practice Model and Framework. June 2010. Final Version 1.0 (U.S.); The U.S. National Cybersecurity Workforce Framework. URL: https://www.dhs.gov/ nationalcybersecurity-workforce-framework (дата обращения: 05.01.2023).

[3] The Cyber Security Capability Framework & Mapping of ISM Roles. Final Report. Australian Government Information Management Office. June 2010.

[4] The European e-Competence Framework 3.0. A common European Framework for ICT Professionals in all industry sectors. CWA 16234:2014 Part 1. CEN.

[5] Национальный стандарт РФ «Информационные технологии. Методы и средства обеспечения безопасности. Требования к компетентности специалистов по системам менеджмента информационной безопасности». URL: http://base.garant.ru (дата обращения: 05.01.2023).

[6] Васильева Д. С., Шабурова А. В. Модель компетентности специалиста по ИБ в современных условиях. URL: https://cyberleninka.ru/article/n/model-kompetentnosti-spetsialista-po-informatsionnoy-bezopasnosti-v-sovremennyh-usloviyah (дата обращения: 15.01.2023).

[7] Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 10.03.01 «Информационная безопасность». URL: http://fgosvo.ru/ (дата обращения: 15.01.2023).

нять нормативно-правовые акты, нормативные и методические документы по ЗИ; организовывать ЗИ ограниченного доступа в соответствии с действующими документами, правовыми актами и законами Федеральной службы безопасности (ФСБ) РФ, Федеральной службы по техническому и экспортному контролю; применять средства криптографической и технической ЗИ; принимать участие в формировании политики ИБ, организовывать и поддерживать выполнение комплекса мер по обеспечению ИБ, управлять процессом их реализации на объекте защиты; проводить подготовку исходных данных для проектирования подсистем ЗИ, средств защиты информации (СЗИ) и технико-экономического обоснования проектных решений.

Рассмотрим требования работодателей к соискателям на должности по ИБ. В число стандартных требований входят: знание нормативно-правовой информации и законодательства по ИБ, сетевых протоколов и стандартов, инструментальных средств организации системной и сетевой безопасности, принципов работы и функциональных возможностей СЗИ и сетевого оборудования для контроля и разграничения доступа, организации защиты от несанкционированного доступа (НСД), обеспечения целостности информации, обнаружения и предотвращения вторжений и анализа защищенности. Кроме того, необходимо изучить методы анализа рисков, технологий, программно-аппаратных и технических СЗИ, порядка проведения аудита ИБ, стандартов шифрования информации, экспертизы по выполнению требований по ИБ и т. д.

Проанализируем обобщенные трудовые функции (ОТФ) из ПС стандартов по ИБ в соответствии с квалификацией бакалавров (уровень 6).

Среди требований ПС «Специалист по безопасности компьютерных систем (КС) и сетей»[1] ОТФ по администрированию СЗИ в КС и сетях включает: работы по администрированию СЗИ в операционных системах (ОС) и КС, заключающиеся в определении программно-аппаратных СЗИ, разработке порядка их применения; формировании и установке программно-аппаратных СЗИ в ОС и шаблонов их конфигурации в КС, в том числе с использованием криптографических методов ЗИ; конфигурирование и контроль за работой программно-аппаратных СЗИ в ОС и КС; управлении антивирусной защитой ОС средствами межсетевого экранирования в КС. ОТФ по администрированию СЗИ прикладного и системного программного обеспечения (ПО) подразумевает определенный порядок установки ПО при соблюдении требований по ЗИ; формулирование требований к параметрам антивирусных средств защиты; выполнение работ по обнаружению и ликвидации вредоносного ПО и последствий его функционирования.

ПС «Специалист по ЗИ в автоматизированных системах (АС)»[2] при осуществлении деятельности по обеспечению ЗИ в АС в процессе их эксплуатации включает: диагностику и администрирование систем ЗИ АС; управление ЗИ в АС; обеспечение

[1] Профессиональный стандарт «Специалист по безопасности компьютерных систем и сетей» [утвержден приказом Министерства труда и социальной защиты РФ от 14 сентября 2022 года №533н.] URL: http://base.garant.ru (дата обращения: 15.01.2023).

[2] Профессиональный стандарт «Специалист по защите информации в автоматизированных системах» [утвержден приказом Министерства труда и социальной защиты РФ от 14 сентября 2022 года №525н.]. URL: http://base.garant.ru (дата обращения: 15.01.2023).

работоспособности систем ЗИ при возникновении нештатных ситуаций; мониторинг и аудит защищенности информации в АС; установку и настройку СЗИ в АС; разработку организационно-распорядительных документов по ЗИ в АС; анализ уязвимостей внедряемой системы; разработку и внедрение мер организационного характера по ЗИ в АС.

ПС «Специалист по технической защите информации (ТЗИ)»[1] в соответствии со стандартом должен выполнять установку, настройку и испытания защищенных средств обработки информации (СОИ), обеспечивать их техническое обслуживание (ТО). Также специалист должен осуществлять производство, сервисное обслуживание, ремонт технических СЗИ, защищенных технических СОИ и контролировать эффективность применяемых мер ЗИ по предотвращению утечки из-за побочных электромагнитных излучений и наводок. Этот стандарт под проведением контроля защищенности информации подразумевает: проведение специальных исследований на побочные электромагнитные излучения и наводки технических СОИ; контроль защищенности информации от утечки за счет побочных электромагнитных излучений и наводок; контроль защищенности акустической речевой информации от утечки по техническим каналам; защиту от НСД.

Нами был проведен анализ ПК, сформулированных в ОП подготовки бакалавров по ИБ, представленных на официальных сайтах нескольких образовательных организаций[2], который показал, что при формулировании ПК вузы в основном руководствовались рассмотренными ранее ПС и включили компетенции, связанные с обслуживанием и администрированием подсистем ЗИ в ОС; обслуживанием и администрированием программно-аппаратных СЗИ в КС; администрированием СЗИ прикладного и системного ПО; проведением анализа безопасности КС и разработкой требований по ЗИ в КС и сетях. Указанные компетенции направлены на формирование следующих способностей: по обеспечению ЗИ в АС в процессе их эксплуатации; по разработке проектных решений по ЗИ в АС; способностей к анализу ИБ объектов и систем на их соответствие требованиям нормативно-методических документов и стандартов в области ИБ; к участию в проведении экспериментальных исследований систем ЗИ; по организации и выполнению комплекса мер по обеспечению ИБ и управлению процессом их реализации; по проведению диагностики СЗИ АС; по администрированию систем ЗИ в АС; к управлению ЗИ в АС; по обоснованию необхо-

[1] Профессиональный стандарт «Специалист по технической защите информации» [утвержден приказом Министерства труда и социальной защиты РФ 9 августа 2022 г. №474н.]. URL: http://base.garant.ru (дата обращения: 15.01.2023).

[2] ФГБОУ ВО «Саратовский государственный технический университет им. Гагарина Ю. А.». URL: https://www.sstu.ru/sveden/document/programms/#10.03.01 (дата обращения: 15.01.2023); ФГБОУ ВО «Национальный исследовательский Мордовский государственный университет им. Н. П. Огарева». URL: https://mrsu.ru/ru/education/graduate/10-03-01-informacionnaya-bezopasnost-ielis/ (дата обращения: 15.01.2023); ФГБОУ ВО «Амурский государственный университет». URL: https://www.amursu.ru/sveden/education/programs/345/ (дата обращения: 15.01.2023); ФГАУ ВО «Казанский (Приволжский) федеральный университет» (КФУ). URL: https://kpfu.ru/computing-technology/uchebnyj-process/karty-kompetencij-2021 (дата обращения: 15.01.2023).

димости ЗИ в АС; по обеспечению работоспособности систем ЗИ при возникновении нештатных ситуаций; по проведению мониторинга защищенности информации в АС; к анализу уязвимостей внедряемой системы ЗИ; к организации и проведению аудита защищенности информации в АС; по установке и настройке СЗИ в АС; к разработке организационно-распорядительных документов по ЗИ в АС; к внедрению организационных мер по ЗИ в АС; к использованию актуальных знаний и современных технологий в профессиональной деятельности.

На основе проведенного анализа нами были определены следующие ПК бакалавров по ИБ (включая индикаторы для их оценки):

1. Способен обеспечивать ЗИ в АС в процессе их эксплуатации: администрирует системы ЗИ АС; обеспечивает их работоспособность при возникновении нештатных ситуаций; осуществляет мониторинг защищенности информации в АС (ПС №525н, ОТФ В, ТФ В/02.6, В/04.6, В/05.6).

2. Способен внедрять системы ЗИ АС: устанавливает и настраивает СЗИ в АС; разрабатывает организационно-распорядительные документы по ЗИ в АС; внедряет организационные меры по ЗИ в АС; анализирует уязвимости внедряемой системы ЗИ (ПС №525н, ОТФ С, ТФ С/01.6, С/02.6, С/03.6, С/04.6).

3. Способен выполнять установку и ТО защищенных технических СЗИ: проводит работы по установке, настройке и испытаниям защищенных технических СОИ и по ТО защищенных технических СЗИ (ПС №474н, ОТФ В, ТФ В/01.6, В/02.6).

4. Способен администрировать СЗИ в КС и сетях: администрирует подсистемы ЗИ в ОС и программно-аппаратные СЗИ в КС (ПС №533н, ОТФ В, ТФ В/01.6, В/02.6).

Сформулированные в данном исследовании ПК находят отражение и в ОП рассмотренных вузов, что подтверждает их актуальность.

Выводы

На основе анализа российских и международных стандартов, публикаций по компетентностному подходу, компетентностной модели специалистов, требований ФГОС ВО по направлению 10.03.01 «Информационная безопасность» в части определения ПК, запроса работодателей, квалификационных требований ПС в данной области были сформулированы ПК бакалавров по ИБ, которые заключаются в способности обеспечивать защиту информации в АС системах в процессе их эксплуатации; осуществлять внедрение систем ЗИ АС; проводить работы по установке и техническому обслуживанию защищенных технических СЗИ; администрировать средства защиты информации в КС и сетях.

Для оценки результатов обучения используются индикаторы достижения (в виде конкретных действий) и дескрипторы (позволяющие оценить сформированность компетенции). Исследователи выделяют разные уровни развития компетенций, например, начальный, базовый, продвинутый. На начальном уровне компетенция частично проявляется в виде действий, входящих в ее состав. Обучающийся проявляет определенные в индикаторах навыки, понимает их необходимость в профессиональной деятельности. Он способен действовать по заданному алгоритму и под руководством преподавателя. На базовом уровне обучающийся овладевает навыками,

необходимыми для решения стандартных ситуаций или ситуаций с элементами неопределённости. На продвинутом уровне важно продемонстрировать способность активно действовать, влиять на происходящие процессы в сложных ситуациях и в условиях неопределенности. Каждый из уровней предусматривает конкретные характеристики мотивационного, когнитивного и деятельностного компонентов, а также их составляющих. Помимо этого, для оценки результатов можно использовать запросы рынка труда в рассматриваемой области профессиональной деятельности, а также квалификационные характеристики, представленные в ПС, на основе которых были сформулированы ПК.

Проведенный анализ ОП подготовки бакалавров по ИБ на основе материалов, представленных на сайтах организаций высшего образования, подтвердил актуальность сформулированных в исследовании ПК с учетом специфики реализуемых профилей. Большинство вузов разрабатывает ПК, основываясь на требованиях ПС, а не исходя из собственного опыта и перспектив развития рынка.

В рассмотренных ОП бакалавров по ИБ сформулированные ПК реализуются в части, формируемой образовательными учреждениями в дисциплинах профессиональной направленности («Администрирование систем защиты информации», «Комплексная защита объектов информатизации», «Защита информационных систем ключевой инфраструктуры» и т. д.), производственных практиках, при написании бакалаврами выпускных квалификационных работ.

При реализации ОП в рамках изучения отдельных дисциплин, модулей, практик в рабочих программах каждый из индикаторов и дескрипторов ПК конкретизируется в виде описания знаний и умений выпускников и опыта практического применения в определенной дисциплине или на практике, в совокупности формируя ПК. Кроме того, результаты обучения оцениваются на основе тестирования когнитивной (теоретической) составляющей (знаний) и практических заданий, значимых для проверки умений и навыков – деятельностной составляющей компетенции. Для оценки допускается использовать и практико-ориентированные кейсы, представляющие собой модели реальных ситуаций, взятых из профессиональной сферы. Они дают обучающемуся возможность продемонстрировать не только действия в стандартных ситуациях, но и в ситуациях неопределенности, которые могут произойти в дальнейшем при осуществлении профессиональной деятельности. Кейсы, не подразумевая конкретного решения поставленной задачи, кроме способа оценки ПК, способствуют развитию мышления, коммуникативных навыков при обосновании своей позиции в выборе того или иного способа решения проблемы и других универсальных и общепрофессиональных компетенций. Использование кейсов повышает мотивацию к изучению дисциплин профессиональной направленности.

Проведенное исследование может быть использовано для классификации ПК в рамках программ подготовки специалистов по ЗИ и бакалавров по другим направлениям подготовки в области ИТ.

Список источников

Анурьева М. С. Направления развития отечественной системы подготовки специалистов по защите информации // Вестник Тамбовского университета. Серия: Естественные и технические науки. 2013. Т. 18. Вып. 1. С. 230–232.

Бурькова Е. В. Профессиональная подготовка специалистов в области информационной безопасности // Вестник Оренбургского государственного университета. 2016. № 2. С. 3–9.

Васильева Д. С., Шабурова А. В. Модель компетентности специалиста по ИБ в современных условиях. URL: https://cyberleninka.ru/article/n/model-kompetentnosti-spetsialista-po-informatsionnoy-bezopasnosti-v-sovremennyh-usloviyah (дата обращения: 15.01.2023).

Доктрина информационной безопасности Российской Федерации. URL: http://base.garant.ru/71556224 (дата обращения: 15.01.2023).

Кобзева Н. И. Профессиональные компетенции в контексте компетентностно-ориентированного подхода в образовании // Вестник Оренбургского государственного университета. 2018. № 5 (217). С. 36–42.

Кравцов А. А. Специфика профессиональной подготовки студентов по направлению «Информационная безопасность» // Вестник Московского государственного лингвистического университета. 2013. № 16 (676). С. 137–149.

Лавина Т. А., Ильина Л. А. ИКТ-компетентность будущих специалистов по защите информации // Вестник Череповецкого государственного университета. 2021. № 6 (105). С. 112–128.

Лавина Т. А., Мытникова Е. А., Давыдова О. В. Профессиональные компетенции бакалавров по направлению «Программная инженерия» // Вестник Череповецкого государственного университета. 2022. № 5 (110). С. 218–226.

Милославская Н. Г., Толстой А. И. Компетентностные требования стандартов ISO/IEC к профессионалам в области информационной безопасности // Безопасность информационных систем. 2017. Т. 24. № 4. С. 6–18.

Национальный стандарт РФ «Информационные технологии. Методы и средства обеспечения безопасности. Требования к компетентности специалистов по системам менеджмента информационной безопасности». URL: http://base.garant.ru (дата обращения: 05.01.2023).

Помельникова Е. А. Формирование готовности будущих специалистов по ИБ к успешной профессиональной деятельности: дис. … канд. пед. наук. Самара: [б. и.], 2019. 183 с.

Профессиональный стандарт «Специалист по безопасности компьютерных систем и сетей» [утвержден приказом Министерства труда и социальной защиты РФ от 14 сентября 2022 года №533н.]. URL: http://base.garant.ru (дата обращения: 15.01.2023).

Профессиональный стандарт «Специалист по защите информации в автоматизированных системах» [утвержден приказом Министерства труда и социальной защиты РФ от 14 сентября 2022 года №525н.]. URL: http://base.garant.ru (дата обращения: 15.01.2023).

Профессиональный стандарт «Специалист по технической защите информации» [утвержден приказом Министерства труда и социальной защиты РФ 9 августа 2022 г. №474н.]. URL: http://base.garant.ru (дата обращения: 15.01.2023).

Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 10.03.01 «Информационная безопасность». URL: http://fgosvo.ru/ (дата обращения: 15.01.2023).

ISO/IEC 27021:2017 "Information technology – Security techniques – Competence requirements for information security management systems professionals", IDT.

State Government Information Security Workforce Development Model. A Best Practice Model and Framework. June 2010. Final Version 1.0 (U.S.)

The U.S. National Cybersecurity Workforce Framework. URL:

https://www.dhs.gov/nationalcybersecurity-workforce-framework (дата обращения: 15.01.2023).

The Cyber Security Capability Framework & Mapping of ISM Roles. Final Report. Australian Government Information Management Office. June 2010.

The European e-Competence Framework 3.0. A common European Framework for ICT Professionals in all industry sectors. CWA 16234:2014 Part 1. CEN.

References

Anur'eva M. S. Napravleniia razvitiia otechestvennoi sistemy podgotovki spetsialistov po zashchite informatsii [Trends of national training of information protection specialists]. *Vestnik Tambovskogo universiteta. Seriia: Estestvennye i tekhnicheskie nauki* [Tambov university reports. Series: Natural and technical sciences], 2013, vol. 18, iss. 1, pp. 230–232.

Bur'kova E. V. Professional'naia podgotovka spetsialistov v oblasti informatsionnoi bezopasnosti [Professional training in the field of information security]. *Vestnik Orenburgskogo gosudarstvennogo universiteta* [Bulletin of Orenburg State University], 2016, no. 2, pp. 3–9.

Doktrina informatsionnoi bezopasnosti Rossiiskoi Federatsii [Information Security Doctrine of the Russian Federation]. Available at: http://base.garant.ru/71556224 (accessed: 15.01.2023).

Federal'nyi gosudarstvennyi obrazovatel'nyi standart vysshego obrazovaniia po napravleniiu podgotovki 10.03.01 «Informatsionnaia bezopasnost'» [Federal state educational standard of higher education in the field of training 10.03.01 "Information security"]. Available at: http://fgosvo.ru/ (accessed: 15.01.2023).

ISO/IEC 27021:2017 "Information technology Security techniques – Competence requirements for information security management systems professionals", IDT.

Kobzeva N. I. Professional'nye kompetentsii v kontekste kompetentnostno-orientirovannogo podkhoda v obrazovanii [Professional competences in the context of a competence-based approach in education]. *Vestnik Orenburgskogo gosudarstvennogo universiteta* [Bulletin of Orenburg State University], 2018, no. (217), pp. 36–42.

Kravtsov A. A. Spetsifika professional'noi podgotovki studentov po napravleniiu «Informatsionnaia bezopasnost'» [Specificity of professional training of students in 'Information Security']. *Vestnik Moskovskogo gosudarstvennogo lingvisticheskogo universiteta* [Vestnik of Moscow State Linguistic University], 2013, no. 16 (676), pp.137–149.

Lavina T. A., Il'ina L. A. IKT-kompetentnost' budushchikh spetsialistov po zashchite informatsii [ICT competence of future information security specialists]. *Vestnik Cherepovetskogo gosudarstvennogo universiteta* [Cherepovets State University Bulletin], 2021, no. 6 (105), pp. 112–128.

Lavina T. A., Mytnikova E. A., Davydova O. V. Professional'nye kompetentsii bakalavrov po napravleniiu «Programmnaia inzheneriia» [Bachelors' professional competencies in the education programme "Software Engineering"]. *Vestnik Cherepovetskogo gosudarstvennogo universiteta* [Cherepovets State University Bulletin], 2022, no. 5 (110), pp. 218–226.

Miloslavskaia N. G., Tolstoi A. I. Kompetentnostnye trebovaniia standartov ISO/IEC k professionalam v oblasti informatsionnoi bezopasnosti [Competence requirements of ISO/IEC standards for information security professionals]. *Bezopasnost' informatsionnykh sistem* [IT Security], 2017, vol. 24, no 4, pp. 6–18.

Natsional'nyi standart RF «Informatsionnye tekhnologii. Metody i sredstva obespecheniia bezopasnosti. Trebovaniia k kompetentnosti spetsialistov po sistemam menedzhmenta informatsionnoi bezopasnosti» [National Standard of the Russian Federation "Information technologies. Security techniques and tools. Requirements for the competence of information security management system specialists"]. Available at: http://base.garant.ru (accessed: 05.01.2023).

Pomel'nikova E. A. *Formirovanie gotovnosti budushchikh spetsialistov po IB k uspeshnoi professional'noi deiatel'nosti* [Development of readiness of future IS specialists for successful professional

activity: Cand. Thesis in Pedagogical Sciences], 2019. 183 p.

Professional'nyi standart «Spetsialist po bezopasnosti komp'iuternykh sistem i setei», utverzhden prikazom Ministerstva truda i sotsial'noi zashchity RF ot 14 sentiabria 2022 goda №533n [Professional standard "Specialist in computer systems and network security", approved by Order No. 533n of the Ministry of Labour and Social Protection of the Russian Federation of 14 September 2022]. Available at: http://base.garant.ru (accessed: 15.01.2023).

Professional'nyi standart «Spetsialist po tekhnicheskoi zashchite informatsii», utverzhden prikazom Ministerstva truda i sotsial'noi zashchity RF 9 avgusta 2022 g. №474n [Professional standard "Specialist in technical protection of information", approved by Order of the Ministry of Labour and Social Protection of the Russian Federation No. 474n, 9 August 2022]. Available at: http://base.garant.ru (accessed: 15.01.2023).

Professional'nyi standart «Spetsialist po zashchite informatsii v avtomatizirovannykh sistemakh», utverzhden prikazom Ministerstva truda i sotsial'noi zashchity RF ot 14 sentiabria 2022 goda №525n [Professional Standard "Specialist in Information Protection in Automated Systems", approved by Order No. 525n of the Ministry of Labour and Social Protection of the Russian Federation, September 14, 2022]. Available at: http://base.garant.ru (accessed: 15.01.2023).

State Government Information Security Workforce Development Model. A Best Practice Model and Framework. June 2010. Final Version 1.0 (U.S.)

The Cyber Security Capability Framework & Mapping of ISM Roles. Final Report. Australian Government Information Management Office. June 2010.

The European e-Competence Framework 3.0. A common European Framework for ICT Professionals in all industry sectors. CWA 16234:2014 Part 1. CEN.

The U.S. National Cybersecurity Workforce Framework. Available at: https://www.dhs.gov/ nationalcybersecurity-workforce-framework (accessed: 15.01.2023).

Vasil'eva D. S., Shaburova A. V. *Model' kompetentnosti spetsialista po IB v sovremennykh usloviiakh* [Competence model of IS specialist in modern conditions]. Available at: https://cyberleninka.ru/article/n/model-kompetentnosti-spetsialista-po-informatsionnoy-bezopasnosti-v-sovremennyh-usloviyah (accessed: 15.01.2023).

Сведения об авторах

Татьяна Ароновна Лавина – доктор педагогических наук, профессор; https://orcid.org/ 0000-0002-7622-2246, tlavina@mail.ru, Чувашский государственный университет им. И. Н. Ульянова (д. 15, пр-т Московский, 428000 Чебоксары, Россия); **Tatyana A. Lavina** – Doctor of Pedagogical Sciences, Professor; https://orcid.org/ 0000-0002-7622-2246, tlavina@mail.ru, I. N. Ulianov Chuvash State University (15, pr. Moskovsky, 428000 Cheboksary, Russia).

Лариса Алексеевна Ильина – аспирант; https://orcid.org/0000-0001-8550-2429, larisai2009@gmail.com, Чувашский государственный университет им. И. Н. Ульянова (д. 15, пр-т Московский, 428000 Чебоксары, Россия); **Larisa A. Ilina** – Postgraduate Student; https://orcid.org/0000-0001-8550-2429, larisai2009@gmail.com, I. N. Ulianov Chuvash State University (15, pr. Moskovsky, 428000 Cheboksary, Russia).

Дмитрий Владимирович Ильин – кандидат физико-математических наук, доцент; https://orcid.org/0000-0003-2179-7429, destr@mail.ru, Чувашский государственный университет им. И. Н. Ульянова (д. 15, пр-т Московский, 428000 Чебоксары, Россия); **Dmitry V. Ilyn** – Candidate of Physical and Mathematical Sciences, Associate Professor; https://orcid.org/0000-0003-2179-7429, destr@mail.ru, I. N. Ulianov Chuvash State University (15, pr. Moskovsky, 428000 Cheboksary, Russia).

Заявленный вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации. Авторы заявляют об отсутствии конфликта интересов.

Contribution of the authors: the authors contributed equally to this article. The authors declare no conflicts of interests.

Статья поступила в редакцию 22.02.2023; одобрена после рецензирования 27.03.2023; принята к публикации 03.04.2023.

The article was submitted 22.02.2023; Approved after reviewing 27.03.2023; Accepted for publication 03.04.2023.