

Кадровое обеспечение образовательных программ в области информационной безопасности: проблемы проектирования и развития¹

Н. Л. Микиденко, С. П. Сторожева, Е. Г. Струкова

Развитие информационных технологий и возрастание цивилизационных рисков и угроз актуализируют вопросы информационной безопасности. Резко возрастает потребность в специалистах в области информационной безопасности. Это требует решения целого ряда управленческих, организационных, содержательных вопросов, связанных с организацией и реализацией образовательных программ по информационной безопасности, в том числе вопросов кадрового обеспечения. В таких условиях развитие кадрового потенциала преподавательского состава, формирование необходимых актуальных знаний и компетенций преподавателей для качественной подготовки будущих специалистов становятся актуальными и востребованными. Массовая переподготовка преподавателей становится важной задачей в обеспечении цифровой экономики специалистами по информационной безопасности. Методологической основой исследования приняты положения социологии образования, отражающие проблемы соответствия потребностей в кадрах для цифровой экономики, импортозамещения и национальной безопасности, количества и качества подготовки специалистов в образовательных организациях высшего профессионального образования. Цель исследования – выявить запросы работодателей на компетенции специалистов по информационной безопасности для формирования профессиональных образовательных программ и запросы преподавателей, занятых в подготовке специалистов по информационной безопасности, на актуальные знания, умения, навыки, наличие которых обеспечит инновационность в подготовке молодых специалистов. Гипотеза исследования: существует рассогласованность запросов со стороны субъектов внешней среды, прежде всего работодателей, и возможностей образовательной системы; существует острая необходимость наращивания кадрового потенциала преподавателей, занятых в подготовке специалистов в сфере информационной безопасности. Причины такого рассогласования связаны с (1) динамичным развитием технологий, появлением и нарастанием киберугроз и киберинцидентов, (2) наличием объективных проблем в развитии кадрового потенциала образовательных организаций (низкая доля молодых кадров, недостаточное взаимодействие образовательных организаций с производственными и научными центрами, недостаточная научная и образовательная мобильность научно-педагогических работников при повышении квалификации).

Запросы работодателей и преподавателей выявлены на основе проведенного авторами эмпирического исследования (осень 2021 г.). В социологическом исследовании, проведенном в форме анкетирования, приняли участие 103 преподавателя и 109 сотрудников предприятий, выполняющих функции по обеспечению информационной безопасности организаций и предприятий (преимущественно СФО). Результаты: выявлены запросы работодателей и преподавателей на актуальные для специалиста по информационной безопасности знания, умения, навыки, актуальные программы повышения квалификации и профессиональной переподготовки. Практическая значимость результатов состоит в том, что исследование позволило выявить проблемы проектирования и дизайна образовательных программ по информационной безопасности, сформулировать рекомендации к проектированию.

¹ Исследование выполнено в рамках государственного задания № 071-03-2022-001.

Ключевые слова: информационная безопасность, кадровый потенциал, преподаватели высшей школы, образовательная программа.

1. Введение

Диверсификация экономики и переход на цифровую траекторию развития в ответ на технологические и цивилизационные вызовы актуализируют вопросы информационной безопасности. Существенная роль в обеспечении процессов цифровизации отводится сотрудникам информационной безопасности, способным работать в условиях высокой неопределенности, нестабильности, сложности, неясности. В докладе Е.Б. Белова (заместитель председателя ФУМО ВО ИБ), И.А. Волошиной (сотрудника ВНИИ труда, Минтруд России) в ходе XVII Всероссийской научно-практической конференции «Информационная безопасность цифровой экономики», проходившей в Новосибирске 12 – 15 октября 2021 г., была представлена ожидаемая среднегодовая потребность в специалистах в области информационной безопасности в 2022–2024 годах по субъектам Сибирского и Дальневосточного федеральных округов в объеме 15200 специалистов ежегодно, а также профессии будущего в сфере информационной безопасности [1].

Прогнозируемый рост потребности в специалистах информационной безопасности и недостаточность образовательных программ по подготовке специалистов в области информационной безопасности делает востребованными образовательные программы по направлению «Информационной безопасности» для преподавателей, которые будут обучать будущих специалистов по информационной безопасности. Массовая переподготовка преподавателей становится важной задачей в обеспечении цифровой экономики специалистами по информационной безопасности.

Исследования последних лет говорят «об острой нехватке кадров по направлению «информационная безопасность» [2, С. 987]. Специалисты отмечают, что «любая деятельность человека в цифровом бытии будь то производственная, социальная, политическая, просто бытовая, не может обойтись без надежной защиты информации и безопасных форм ее использования» [3, С. 697]. Подготовка кадров для сферы информационной безопасности широко обсуждается в профессиональном сообществе в разных аспектах: проектирование содержания образовательных курсов и программ [2, 4, 5, 6]; сравнение российских и международных подходов к стандартизации профессиональной и образовательной деятельности в сфере ИТ и основные принципы модели SFIA как наднационального инструмента для описания и управления компетенциями специалистов – разработчиков и эксплуатантов систем на базе ИКТ [7, С. 133]; подготовка педагогов для их реализации и востребованность программ повышения квалификации [8]. Отдельной проблемой обсуждаются компетенции специалистов по информационной безопасности [9], этические проблемы информационной безопасности и подготовка ИТ-специалистов, инновационно-профессионально-этическая проблематика информационной безопасности в VUCA-мире [10, 11, 12] и др. Подчеркивается, что «проблема защиты информации становится личным, деловым и национальным приоритетом и в той или иной мере затрагивает каждого члена общества» [13]. Потребность в кадрах в сфере информационной безопасности испытывается в экономике в целом [14] и в разных ее отраслях [15]. Отмечено, что зачастую «информационная безопасность отстает в развитии от других сфер экономики и в какой-то степени является ее тормозом» [16, С. 116]. Действующие специалисты по информационной безопасности, формулируя требования к профессиональным знаниям, умениям и навыкам будущего профессионала, помимо знаний программно-аппаратного обеспечения средств информационной защиты, нормативно-правовой базы, отмечают значимость таких составляющих, как управленческие и коммуникативные навыки, а также знания методов оценки и прогнозирования поведения человека [17].

На конференции «Кибербезопасность: защита информации как драйвер роста российского бизнеса», проведенной компанией Мегафон 21 июля 2022 года, отмечается, что в первые месяцы 2022 года число кибератак на российский бизнес выросло в четыре раза по сравнению с аналогичным периодом 2021 года, многие компании понесли финансовый и репутационный ущерб. «Задача обеспечения киберзащиты компаний вышла на первый план и напрямую влияет на экономику компаний и достижение бизнес-целей» [18].

В Решении XXVI Пленума ФУМО в системе высшего образования по УГСНП 10.00.00 «Информационная безопасность», прошедшего в рамках Форума информационной безопасности «Сибирь – Дальний Восток 2022» 28 июня – 2 июля 2022 года в Хабаровске, рекомендовано организовать в рамках ФУМО ВО ИБ с привлечением работодателей дискуссию по вопросам структуры и развития номенклатуры образовательных программ в области информационной безопасности, а также развития национальной системы подготовки кадров в области информационной безопасности [19].

Условием развития сферы информационной безопасности является создание специальных профессиональных образовательных программ. Их реализация напрямую зависит от готовности и квалификационных характеристик профессорско-преподавательского состава и актуализирует задачи профессиональной переподготовки и повышения квалификации в этой области.

2. Результаты исследования

2.1. Методология и методика исследования

Для выявления запроса со стороны преподавателей на программы повышения квалификации в сфере информационной безопасности проведено исследование (декабрь 2021 г.). Исследование проведено методом анкетирования с использованием электронной формы анкеты, включавшей три раздела и 30 вопросов. Дизайн анкеты включал следующие тематические блоки: социально-демографическая информация, оценка преподавателями и представителями образовательных организаций состояния рынка труда и востребованных компетенций в области «Информационная безопасность», оценки востребованности программ профессиональной переподготовки и повышения квалификации в области «Информационная безопасность».

2.2. Выборка исследования

Выборка исследования – целевая, неслучайная. В исследовании принимали участие преподаватели, работающие в высших и средних профессиональных образовательных организациях, преподающие дисциплины по образовательным программам в сфере информационной безопасности и проходившие курсы повышения квалификации и/или профессиональную переподготовку в период с сентября по ноябрь 2021 года. Опрос проводился в декабре 2021 года. В исследовании приняли участие 103 человека, среди которых мужчины составили 58.3 %, женщины – 41.2 %. В опросе приняли участие преподаватели 14 образовательных организаций высшего профессионального образования Сибирского федерального округа.

87.4 % участников опроса преподают учебные курсы по образовательным программам направления подготовки «Информационная безопасность». На рис. 1 отражено распределение преподавателей по дисциплинам, которые они преподают. Среди участников опроса более 60 % преподавателей по компьютерным и/или техническим наукам, 16.5 % преподавателей физико-математических дисциплин. В выборке представлены также преподаватели социальных (3.9 %), естественных (3.9 %), экономических (4.9 %) и юридических дисциплин (2.9 %) (рис. 1).

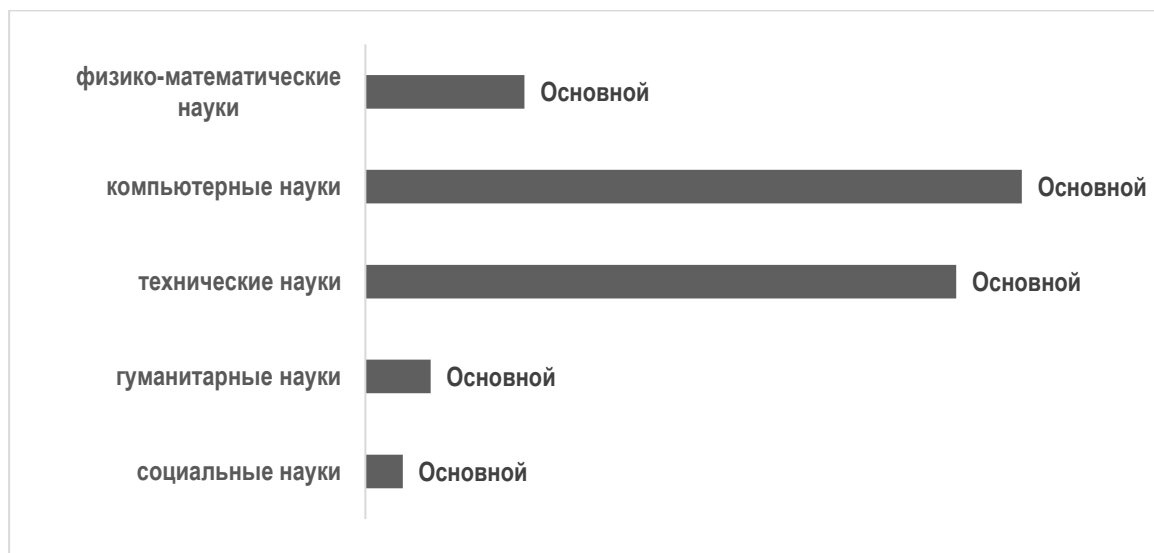


Рис. 1. Сферы науки, к которым относятся дисциплины, преподаваемые участниками опроса (вопрос с множественным выбором, допускается более одного ответа)

Преподаваемые дисциплины развивают разные типы компетенций. 43.7 % опрошенных преподают дисциплины, развивающие универсальные компетенции, 70.9 % – общепрофессиональные, 59.2 % – профессиональные. Распределение ответов отражено на рис. 2.

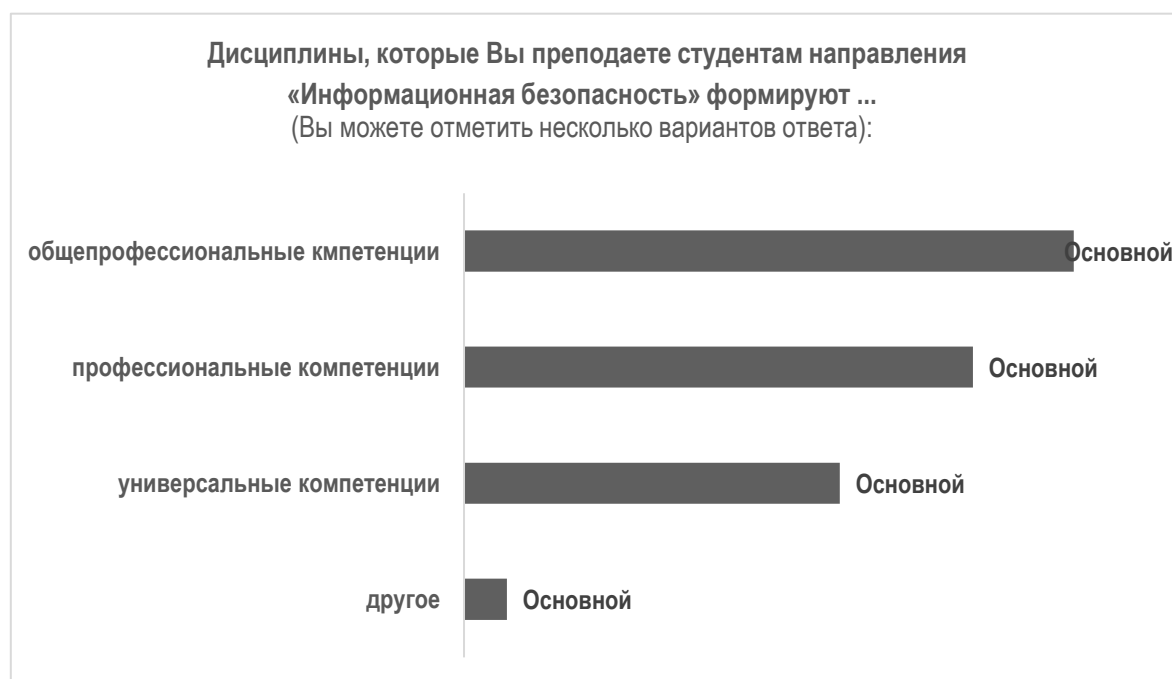
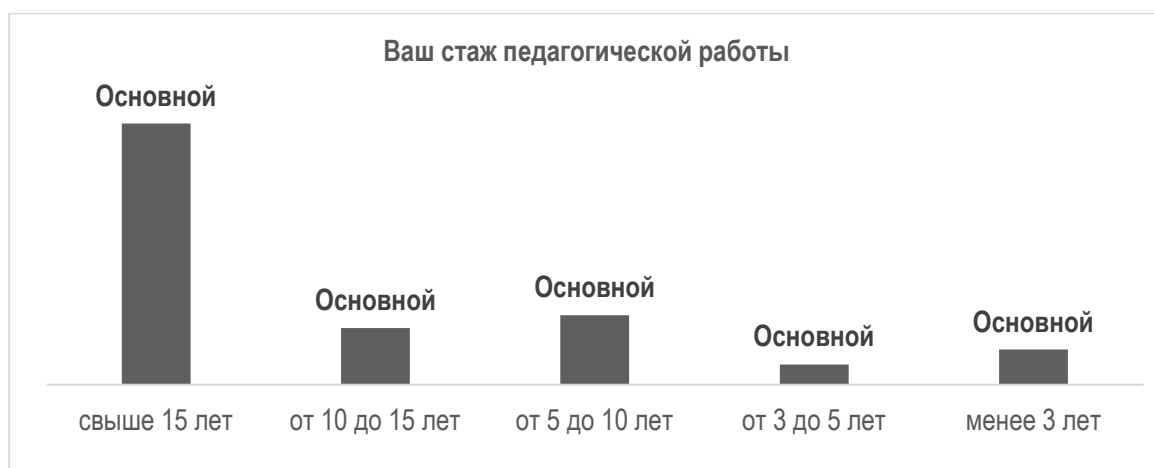


Рис. 2. Компетенции, формируемые дисциплинами преподавателей – участников опроса (% респондентов, вопрос с множественным выбором, допускается более одного ответа)

В опросе приняли участие разные группы преподавателей по стажу научно-педагогической деятельности. 58.3 % имеют стаж работы более 15 лет. Объем групп преподавателей по стажу работы представлен на рис. 3.

Рис. 3. Стаж педагогической работы респондентов ($n = 103$, %)

Респонденты, участвовавшие в опросе, участвуют в реализации разных направлений программ в сфере информационной безопасности (рис. 4):

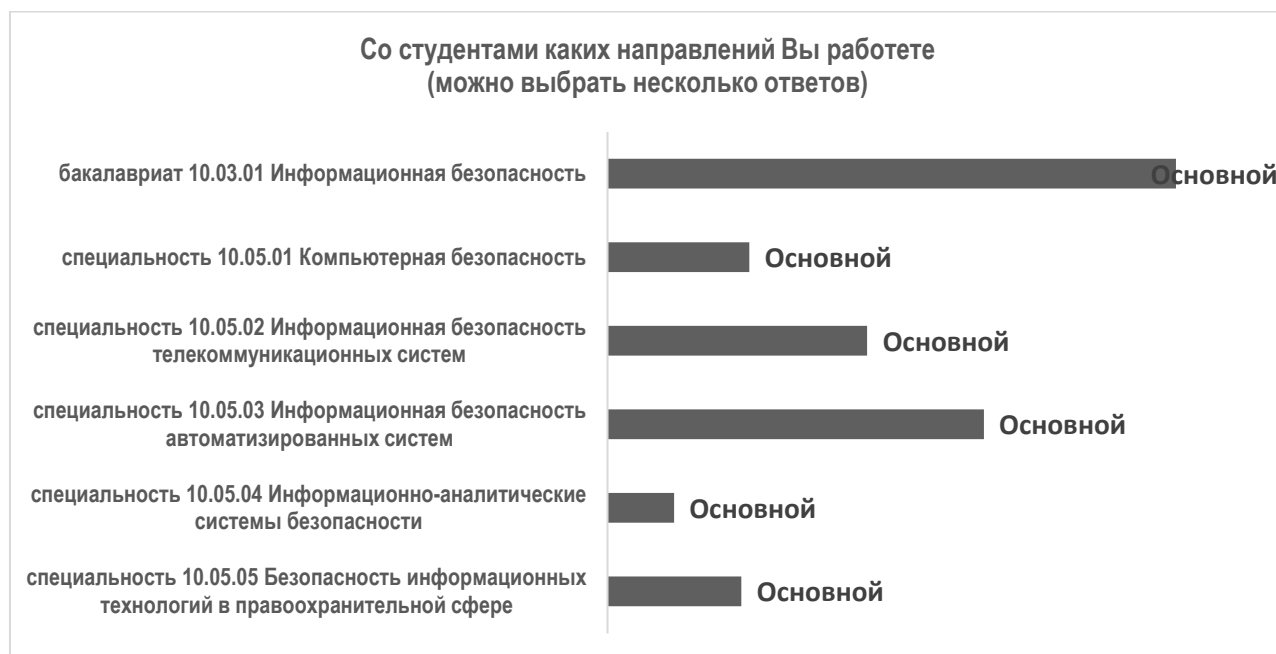


Рис. 4. Образовательные программы, в реализации которых участвуют респонденты (вопрос с множественным выбором, допускается более одного ответа) (% , $n = 97$)

Распределение групп респондентов по преподаваемым дисциплинам, формируемым компетенциям, стажу педагогической работы, региону работы и образовательным программам, в реализации которых они принимают участие, позволяет говорить о том, что в выборке представлены различные группы, что, в свою очередь, позволяет сделать заключение о довольно высокой репрезентативности результатов и целесообразности их использования при формировании предложения по программам повышения квалификации и переподготовки в области «Информационная безопасность».

2.3. Оценки работодателей и преподавателей востребованности компетенций специалиста по информационной безопасности

Преподаватели отмечают, что специалисты по информационной безопасности востребованы на рынке труда. Около 80 % полагают, что существует дефицит таких специалистов (рис. 5).

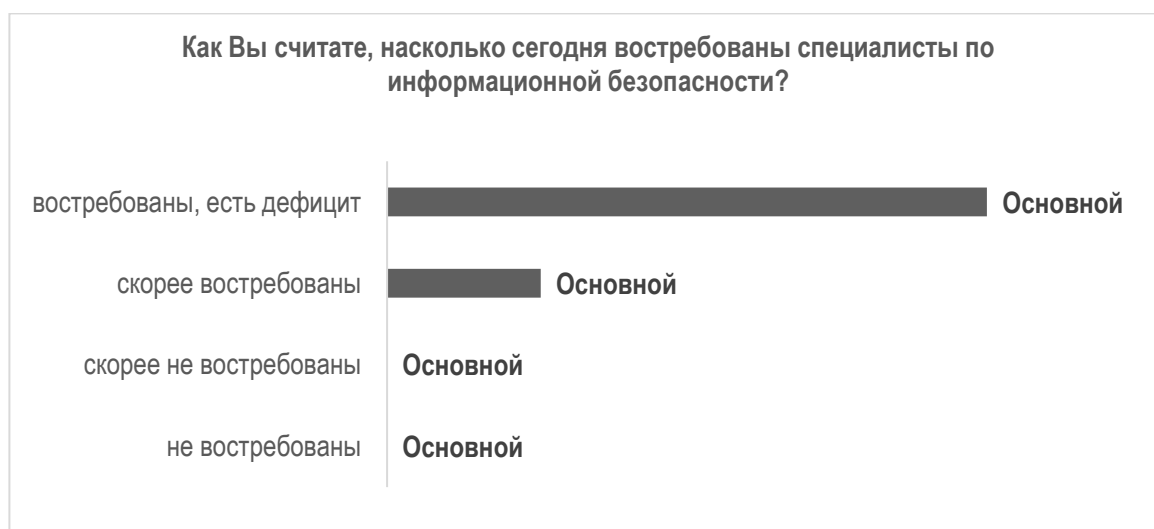


Рис. 5. Мнения преподавателей о востребованности специалистов в области информационной безопасности на рынке труда (% , $n = 103$)

30 % регулярно отслеживают изменения на рынке труда и еще 42 % отмечают, что обращают внимание на то, какие требования работодатели предъявляют к молодым специалистам в области информационной безопасности (рис. 6).

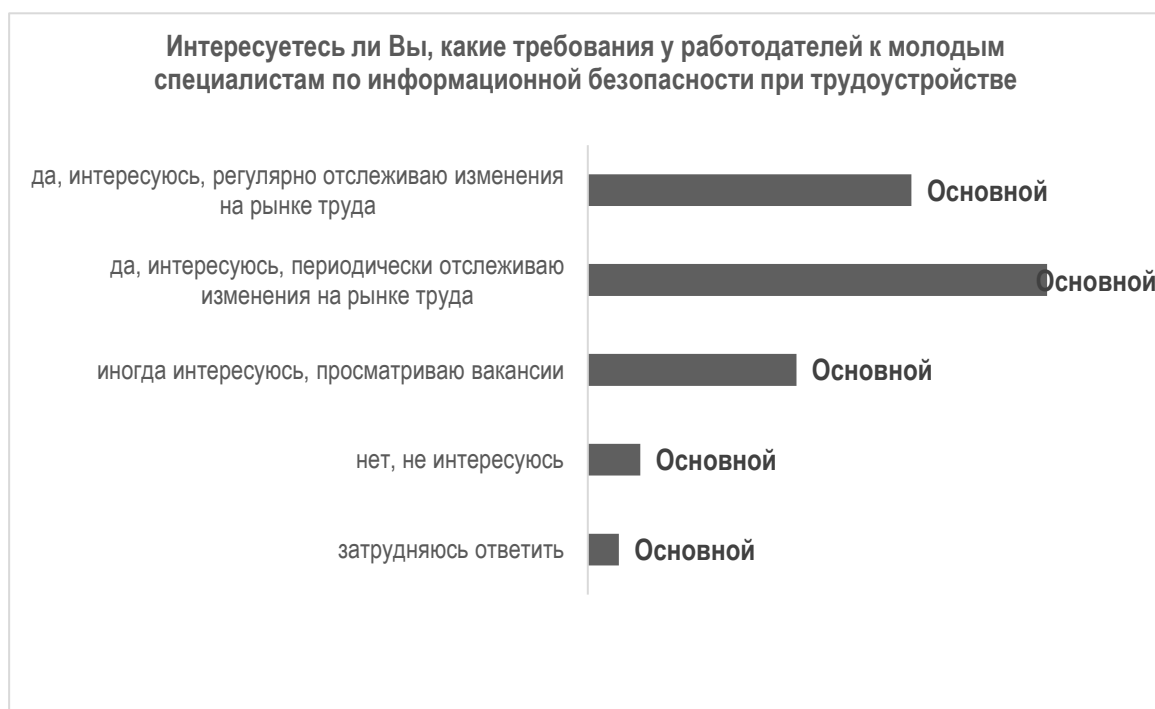


Рис. 6. Представления преподавателей о состоянии рынка труда в области информационной безопасности (% , $n = 103$)

Преподавателям было предложено оценить свои знания о трудовых функциях специалистов по информационной безопасности. Распределение оценок представлено на рис. 7.

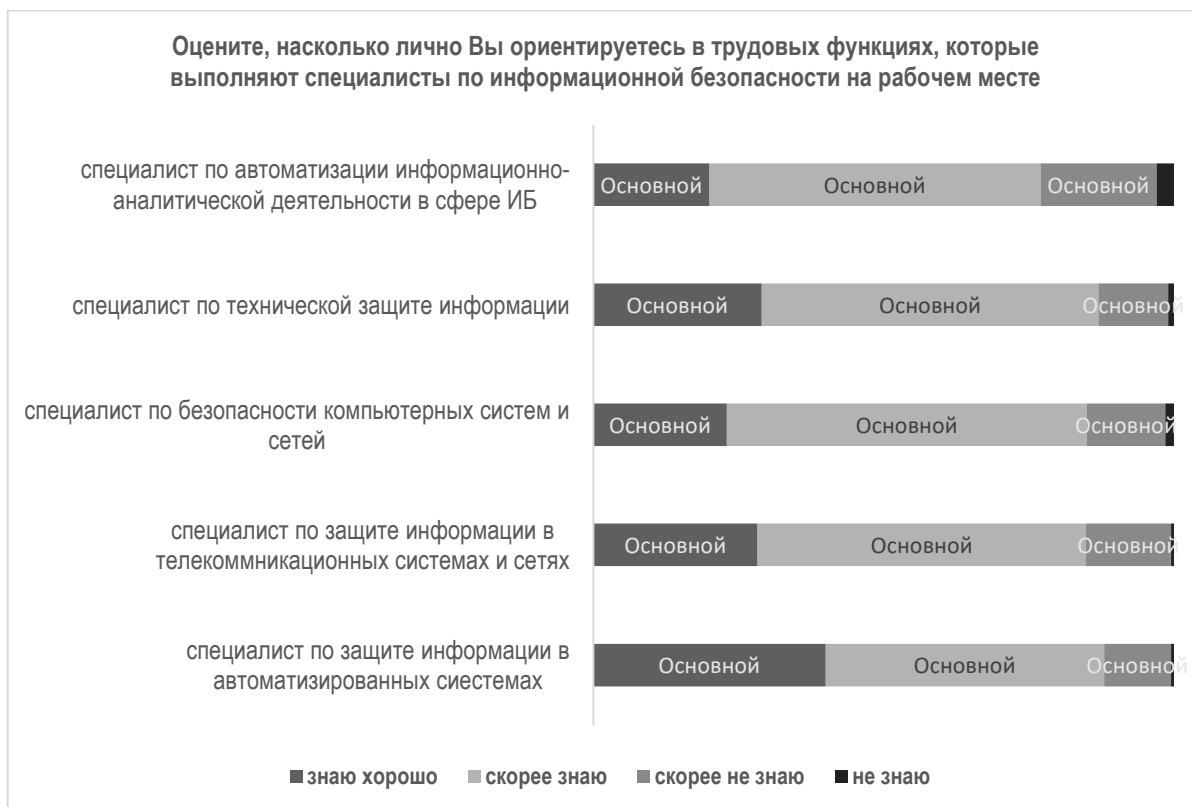


Рис. 7. Представления преподавателей о трудовых функциях специалистов в сфере информационной безопасности (% , $n = 103$)

Также преподавателям было предложено ответить на вопрос о том, насколько достаточно их личных знаний, умений и навыков для организации профессиональной деятельности в подготовке специалистов информационной безопасности (распределение ответов – на рис. 8).

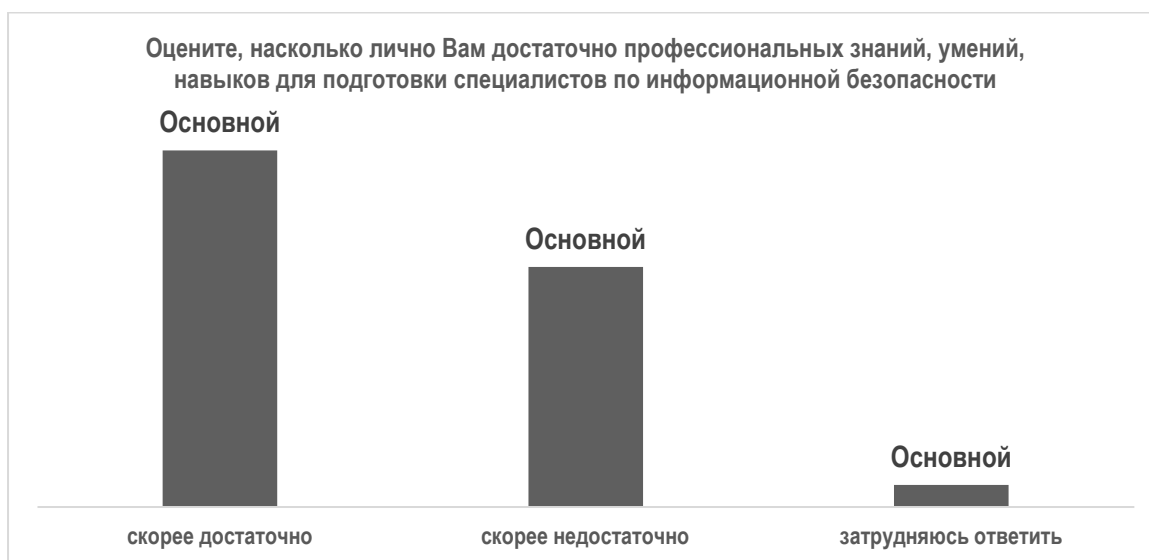


Рис. 8. Самооценка знаний, умений и навыков преподавателей, необходимых для подготовки специалистов по информационной безопасности (% , $n = 103$)

Почти 40 % участников опроса отметили, что им недостаточно знаний, умений и навыков для подготовки специалистов по информационной безопасности (рис. 8). Более 90 % хотели бы пройти повышение квалификации (рис. 9).

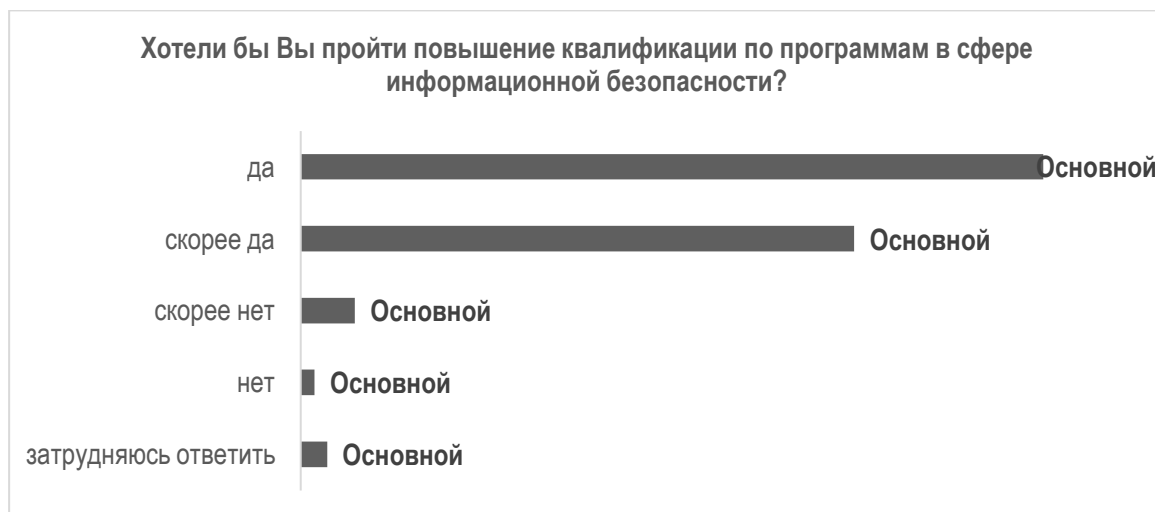


Рис. 9. Оценка потребности в обучении и/или повышении квалификации (% , n = 103)

В табл. 1 отражено распределение предпочтений преподавателей по продолжительности и формам программ обучения. Наибольший интерес представляют программы обучения продолжительностью 72 часа и мастер-классы по отдельным ситуациям в информационной безопасности.

Таблица 1. Предпочтения респондентов по программам повышения квалификации (вопрос с множественным выбором, допускается выбор более одного ответа)

	Программы повышения квалификации (по объему часов)	N (человек)	%
1.	Повышение квалификации в объеме 36 ч.	30	29.1
2.	Повышение квалификации в объеме 72 ч.	57	55.3
3.	Повышение квалификации в объеме 144 ч.	30	29.1
4.	Программа профессиональной переподготовки в объеме более 250 ч.	26	25.2
5.	Мастер-классы по отдельным ситуациям в информационной безопасности	47	45.8
6.	Стажировка на предприятии	28	27.2

Высокий интерес преподаватели проявляют к краткосрочным видам обучения с участием отраслевых предприятий, а также к таким формам повышения квалификации, как тематические мастер-классы по отдельным ситуациям в информационной безопасности (45,8 %) и стажировка на предприятии (27,2 %). На развитие этих форм сотрудничества направлены и предложения по модернизации программ в области ИТ, где предлагается реализовать «возможности совместно с вузами модернизировать учебные программы, проводить совместные практики, привлекать к преподаванию представителей отрасли» (директор по развитию региональных образовательных проектов компании «Яндекс» С. Бражник); а также «участие работодателей в формировании образовательной повестки может проходить, во-первых, через их вовлечение в разработку и актуализацию ФГОС» и «развитие новых форматов партнерства», которые становятся возможны на основе Положения о практической подготовке обучающихся от 5 августа 2020 г. (заместитель министра науки и высшего образования РФ Д. Афанасьев) [20].

Для выявления востребованности тематики программ повышения квалификации по информационной безопасности респондентам предложен примерный перечень программ с возможностью выбрать все интересующие их программы. В табл. 2 отражена востребованность программ согласно предложенной примерной тематике.

Таблица 2. Востребованность у преподавателей программ повышения квалификации по информационной безопасности

Примерная тематика программ повышения квалификации по информационной безопасности	№ респондентов, которые выразили интерес к программе
10.03.01 Информационная безопасность. Базовые дисциплины	
1. Основы информационной безопасности	19
2. Сети и системы передачи информации	17
3. Программно-аппаратные средства защиты информации	27
4. Основы управления информационной безопасностью	30
5. Защита информации от утечки по техническим каналам	26
6. Методы и средства криптографической защиты информации	31
7. Организационное и правовое обеспечение информационной безопасности	24
8. Комплексная защита объектов информатизации	34
10.03.01 Информационная безопасность. Профессиональные дисциплины	
1. Безопасность операционных систем	21
2. Защита в операционных системах	19
3. Криптографические протоколы	20
4. Безопасность систем баз данных	20
5. Основы построения защищенных компьютерных сетей	20
6. Методы оценки безопасности компьютерных систем	35
7. Безопасность вычислительных сетей	16
8. Безопасность информационной инфраструктуры	20
9. Проектирование защищенных автоматизированных систем	28
10. Математическое моделирование систем и сетей телекоммуникаций	15
11. Проектирование элементов защищенных телекоммуникационных систем	10
12. Документоведение и конфиденциальное делопроизводство	16
13. Методы принятия организационно-технических решений	18
14. Моделирование процессов и систем защиты информации	21

15. Основы построения и функционирования специальных технических средств	6
16. Защита информации от несанкционированного доступа	30
17. Основы проектирования систем защиты объектов информатизации	22
10.05.01 Компьютерная безопасность. Базовые дисциплины	
1. Криптографические методы защиты информации	22
2. Защита в операционных системах	15
3. Основы построения защищенных баз данных	17
4. Защита программ и данных	18
5. Модели безопасности компьютерных систем	27
6. Криптографические протоколы	20
10.05.01 Компьютерная безопасность. Профессиональные дисциплины	
1. Анализ безопасности компьютерных систем	19
2. Математические методы защиты информации	18
3. Разработка защищенного программного обеспечения	17
4. Безопасность компьютерных систем и сетей (по отрасли или в сфере профессиональной деятельности)	15
5. Разработка систем защиты информации компьютерных систем объектов информатизации (по отрасли или в сфере профессиональной деятельности)	15
6. Информационно-аналитическая и техническая экспертиза компьютерных систем	28
10.05.02 Информационная безопасность телекоммуникационных систем. Базовые дисциплины	
1. Сети и системы передачи информации	14
2. Моделирование систем и сетей телекоммуникаций	13
3. Методы и средства криптографической защиты информации	15
4. Программно-аппаратные средства защиты информации телекоммуникационных систем	16
5. Комплексное обеспечение защиты информации телекоммуникационных систем	20
6. Проектирование защищенных телекоммуникационных систем	18
10.05.02 Информационная безопасность телекоммуникационных систем. Профессиональные дисциплины	
1. Информационная безопасность аэрокосмических ТКС	9
2. Разработка защищенных ТКС	14

3. Защита информации в радиосвязи и телерадиовещании	8
4. Управление безопасностью ТКСиС	7
5. Информационная безопасность мультисервисных телекоммуникационных сетей и систем на транспорте (по видам)	7
6. Системы подвижной цифровой защищенной связи	13
7. Техническая защита информации информационно-телекоммуникационных систем	19
10.05.03 Информационная безопасность автоматизированных систем. Базовые дисциплины	
1. Безопасность операционных систем	20
2. Безопасность вычислительных сетей	16
3. Безопасность систем баз данных	18
4. Управление информационной безопасностью	27
5. Разработка и эксплуатация автоматизированных систем в защищенном исполнении	24
6. Программно-аппаратные средства защиты информации	26
10.05.03 Информационная безопасность автоматизированных систем. Профессиональные дисциплины	
1. Безопасность открытых информационных систем	16
2. Безопасность автоматизированных систем в финансово-кредитной сфере	17
3. Анализ безопасности информационных систем	26
4. Разработка автоматизированных систем в защищенном исполнении	18
5. Безопасность автоматизированных систем на транспорте (по видам)	6
6. Безопасность автоматизированных систем управления технологическими процессами (по отрасли или в сфере профессиональной деятельности)	11
7. Безопасность значимых объектов критической информационной инфраструктуры (по отрасли или в сфере профессиональной деятельности)	27
10.05.04 Информационно-аналитические системы безопасности. Базовые дисциплины	
1. Безопасность информационно-аналитических систем	11
2. Базы данных и экспертные системы	16
3. Распределённые информационно-аналитические системы	11
4. Моделирование автоматизированных информационно-аналитических систем	7
5. Технологии интеллектуальной обработки и анализа текстовых и мультимедийных данных	9
6. Обработка данных больших объемов	17

7. Принципы построения, проектирования и эксплуатации информационно-аналитических систем	13
10.05.04 Информационно-аналитические системы безопасности. Профессиональные дисциплины	
1. Автоматизация информационно-аналитической деятельности	16
2. Информационная безопасность финансовых и экономических структур	19
3. Технологии информационно-аналитического мониторинга	19
10.05.05 Безопасность информационных технологий в правоохранительной сфере. Базовые дисциплины	
1. Теория информационной безопасности и методология защиты информации	13
2. Информационное право	11
3. Защита и обработка документов ограниченного доступа	10
4. Организационная защита информации	13
5. Инженерно-техническая защита	8
6. Специальные информационные технологии в правоохранительной деятельности	14
7. Компьютерная криминалистика	30
10.05.05 Безопасность информационных технологий в правоохранительной сфере. Профессиональные дисциплины	
1. Компьютерная экспертиза	36
2. Организация и технологии обеспечения защиты информации	30

Ответы респондентов отражают востребованность широкого круга программ и дисциплин для бакалавриата и специалитета по базовым и профессиональным дисциплинам в области информационной безопасности.

Также преподавателям было предложено оценить востребованность дополнительных знаний, связанных с умением выстраивать педагогические и учебные процессы в цифровой образовательной среде, недостаточность которых остро ощущалась в период экстренного перехода в онлайн-формат обучения. Многочисленные исследования показывали серьезные сложности, которые возникли в организации учебных занятий, связанные именно с недостаточностью цифровых компетенций преподавателей. Так, в аналитическом докладе «Уроки стресс-теста» отмечено, что доля преподавателей, которые не смогли освоить цифровые инструменты работы, составила от 5 до 30 % в зависимости от вуза [21, С. 17]. При этом «дистанционный формат воспринимается как тотальное противопоставление традиционному по принципу «черное-белое». При жестком сравнении почти 90 % преподавателей отдадут предпочтение традиционному формату с точки зрения качества образования, а 85 % считают традиционный формат более комфортным для себя» [21, С. 18]. Ответы преподавателей о востребованности обучения навыкам работы в цифровой образовательной среде представлены на рис. 10.

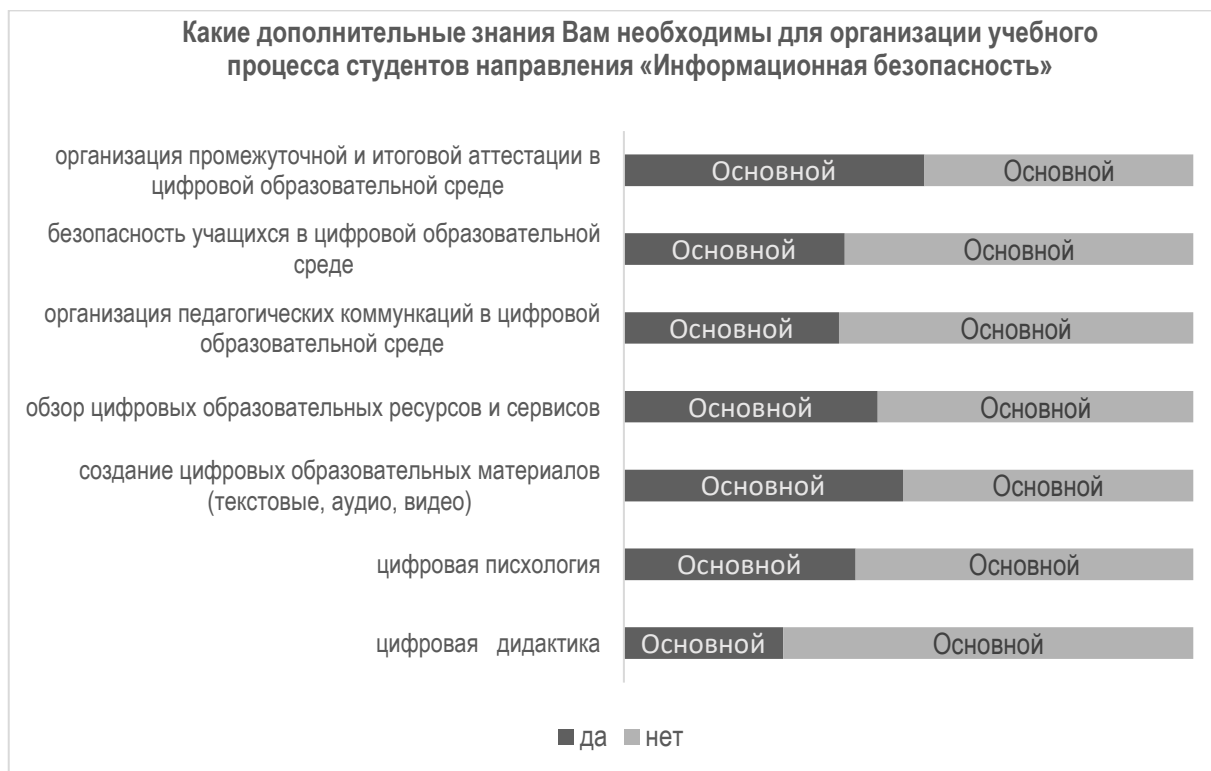


Рис. 10. Потребность в педагогических знаниях, необходимых для реализации учебного процесса для (% , $n = 103$)

Ответы отражают наличие потребности у преподавателей в развитии цифровых компетенций в организации педагогического и учебного процессов в цифровой образовательной среде, что выступает точкой роста педагогического сообщества. Подготовка специалистов по информационной безопасности без использования цифровых образовательных ресурсов и сервисов невозможна. Важны и востребованы также цифровые педагогические компетенции.

3. Заключение

Программы повышения квалификации по информационной безопасности по разной тематике востребованы. Преподаватели отдают предпочтение программам повышения квалификации в объеме 72 часов, мастер-классам и кейсам по отдельным ситуациям. Около 40 % респондентов отмечают недостаточность личных профессиональных знаний, умений и навыков, более 90 % выражают желание пройти повышение квалификации.

В целом преподаватели отмечают свою информированность о трудовых функциях специалистов по информационной безопасности (от 75 до 87 % в зависимости от специализации специалиста по информационной безопасности).

В условиях высокой востребованности специалистов по информационной безопасности и устаревания наличных компетенций необходима организация повышения квалификации преподавателей на регулярной основе при одновременном мониторинге сформированности цифровых компетенций и запросов преподавателей на повышение квалификации с целью выявления точек роста и организации опережающего обучения. Кроме того, необходим мониторинг запроса работодателя на компетенции выпускника образовательной программы.

Литература

1. Подведены итоги Пленума регионального отделения ФУМО по информационной безопасности. Режим доступа: <https://sibsutis.ru/news/3701575/>.
2. Зива С. В., Захаров Д. И. Принципы построения и опыт реализации учебного курса «Прикладные вопросы информационной безопасности» // Современные информационные технологии и ИТ-образование. 2020. Т. 16, № 4. С. 980–989. DOI 10.25559/SITITO.16.202004.980-989.
3. Сухомлин В. А., Белякова О. С., Климина А. С., Полянская М. С., Русанов А. А. Модель цифровых навыков кибербезопасности 2020 // Современные информационные технологии и ИТ-образование. 2020. № 16 (3). С. 695–710. DOI 10.25559/SITITO.16.202003.695-710.
4. Авдеева Е. С., Миронова В. В. Формирование групп стратегических профессий как один из инструментов достижения стратегической конкурентоспособности предприятий // Известия Юго-Западного государственного университета. Серия: Экономика. Социология. Менеджмент. 2017. Т. 7, № 2(23). С. 148–160.
5. Цацкина Е. П., Ляхова Е. Г., Мороз Н. Ю. О лингвистической подготовке кадров по информационной безопасности на этапе перехода к цифровой экономике // Обзор педагогических исследований. 2021. № 3 (6). С. 162–167.
6. Сухомлин В. А., Белякова О. С., Климина А. С., Полянская М. С., Зубарева Е. В., Якушин А. В. Архитектура и принципы разработки куррикулума для дисциплины «Кибербезопасность» // Современные информационные технологии и ИТ-образование. 2020. № 16(4). С. 927–939.
7. Дрожжинов В. И. SFIA-система профессиональных стандартов в сфере ИТ эпохи цифровой экономики // Современные информационные технологии и ИТ-образование. 2017. № 13 (1). С. 132–143.
8. Цветкова О. Н. Информационная безопасность в условиях цифровой экономики в России // Самоуправление. 2021. № 5 (127). С. 440–443.
9. Малюк А. А., Полянская О. Ю. Комментарии к Доктрине информационной безопасности Российской Федерации. М.: Горячая линия – Телеком, 2018. 102 с. ISBN 978-5-9912-0711-9.
10. Малюк А. А., Полянская О. Ю. Этика в сфере информационных технологий // Вестник Российского гуманитарного научного фонда. 2011. № 4 (65). С. 72–77.
11. Профессиональная этика инженера: Опыт коллективной рефлексии для магистр(ант)ов и профессоров: коллективная монография / под ред. В.И. Бакштановского; составители А. Ю. Согомонов, М. В. Богданова. Тюмень: НИИ ПЭ ТИУ, 2018. 246 с.
12. Olifirov A. V., Makoveichuk K. A., Petrenko S. A. Improving the courses of educational programs on information security smart grid // CEUR Workshop Proceedings: 4, Yalta, Crimea, 16–21 Sept. 2019, Yalta, Crimea, 2021. P. 340–350.
13. Малюк А. А., Малюк З. П. Актуальные вопросы создания системы массового обучения культуре информационной безопасности // Безопасность информационных технологий. 2021. № 28 (4). С. 6–21. DOI 10.26583/bit.2021.4.01.
14. Бушуев А. Л., Деревцова И. В., Мальцева Ю. А., Терентьева В. Д. Роль информационной безопасности в условиях цифровой экономики // Baikal Research Journal. 2020. № 11 (1). С. 6. DOI 10.17150/2411-6262.20.11(1).6.
15. Пилипенко В. В., Кузнецова М. А. Анализ российского рынка информационной безопасности в контексте развития цифровой экономики // Инновационная экономика. 2019. № 3 (20). С. 4–12.
16. Антонова Н. Л., Бабикина И. И. Информационная безопасность в условиях цифровой экономики // Заметки ученого. 2020. № 13. С. 111–117.
17. Струкова Е. Г., Микиденко Н. Л., Сторожева С. П. Взаимодействие с работодателем как инструмент формирования образовательной программы // Информационная безопасность цифровой экономики: Материалы XVII научно-теоретической конференции VIII Пленума регионального отделения Федерального учебно-методического объединения в системе

- высшего образования по укрупненной группе специальностей и направлений подготовки 10.00.00 «Информационная безопасность» по Сибирскому и Дальневосточному федеральным округам (СибРОУМО), Новосибирск, 13–15 октября 2021 года. Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2021. С. 78–94.
18. Кибербезопасность: защита информации как драйвер роста бизнеса // Сайт: Мегафон (megafon.ru). URL: Кибербезопасность: защита информации как драйвер роста бизнеса (megafon.ru) (дата обращения: 28.08.2022).
 19. В Хабаровске проходит форум информационной безопасности «Сибирь – Дальний Восток-2022» 30.06.2022 // Сайт: Министерство образования и науки Хабаровского края. URL: <https://minobr.khabkrai.ru/events/Novosti/3606> (дата обращения: 28.08.2022).
 20. Батанов А., Брылякова М. От цифровизации – к аккредитационной революции. Репортаж с парламентских слушаний в Комитете Госдумы РФ по образованию и науке. Апрель. 2022 // Сайт: Аккредитация в образовании. URL: <https://akvobr.ru/new/publications/273> (дата обращения: 28.08.2022).
 21. Аналитический доклад «Уроки стресс-теста: российские вузы в условиях пандемии и после нее». Июнь, 2020. URL: 003_Доклад.pdf (yandex.ru) (дата обращения: 28.08.2022).

*Статья поступила в редакцию 08.08.2022;
переработанный вариант – 30.08.2022.*

Микиденко Наталья Леонидовна

кандидат социологических наук, доцент кафедры социально-коммуникативных технологий, Сибирский государственный университет телекоммуникаций и информатики (630102, Новосибирск, ул. Кирова, 86), тел. (383) 2-693-929, e-mail: nl_nsk@mail.ru.

Сторожева Светлана Петровна

кандидат культурологии, доцент кафедры социально-коммуникативных технологий, Сибирский государственный университет телекоммуникаций и информатики, e-mail: s_storozheva@sibguti.ru.

Струкова Елена Геннадьевна

начальник управления маркетинга и развития образования, Сибирский государственный университет телекоммуникаций и информатики (630102, Новосибирск, ул. Кирова, 86), e-mail: strukova@sibguti.ru.

Staff assistance of educational programs in the sphere of information security: design and development problems

Natalia L. Mikidenko

Candidate of Sociology, Assistant Professor, Assistant Professor Department of Social and Communication Technology (SibSUTIS, Novosibirsk, Russia), nl_nsk@mail.ru.

Svetlana P. Storozheva

Candidate of Culturology, Assistant Professor, Assistant Professor Department of Social and Communication Technology (SibSUTIS, Novosibirsk, Russia), s_storozheva@sibguti.ru.

Elena G. Strukova

Head of Marketing and Education Development Department (SibSUTIS, Novosibirsk, Russia), strukova@sibguti.ru.

An increase in civilization risks and threats, and the development of information technologies actualize the questions of information security. The need for information security specialists is sharply increasing. This requires the solution of a number of managerial, organizational, substantive issues related to the organization and implementation of educational programs on information security including staffing issues. In such conditions the issues of teaching staff potential development, formation of the necessary up-to-date knowledge and competences of teachers for qualitative training of future specialists become urgent and in-demand. Mass retraining of teachers becomes the most important task in providing information security specialists for the digital economy. The methodological basis of the study is the provisions of education sociology reflecting the problems of matching the human resources needs for the digital economy, import substitution and national security with the quantity and quality of specialist training in higher educational institutions of vocational education.

The aim of the research is to identify employers' demands for information security specialists' competences for formation of professional educational programs and demands of teachers engaged in information training for actual knowledge, abilities, skills, which availability will ensure innovativeness in training of young specialists. The main hypothesis was that there is a mismatch between the demands of the external environment of higher education, above all, employers and the capabilities of the educational system, there is an urgent need to increase the capacity of teachers involved in training professionals in the field of information security. The reasons for this mismatch are (1) the dynamic development of technology, the emergence and increase of cyber threats and cyber incidents, (2) the presence of objective problems in the development of educational institutions staff capacity - the low proportion of young personnel, inadequate interaction between educational institutions and industrial and research centers, inadequate scientific and educational mobility of teaching staff for skills development.

The needs of employers and teachers have been identified on the basis of empirical research (autumn, 2021) conducted by the authors. 103 teachers and 109 employees of enterprises which carry out functions on maintenance of information security of organizations and enterprises (mainly SFD) participated in sociological research.

Results: requirements of employers and teachers on information security actual knowledge, abilities, actual programs of professional development and professional retraining were revealed. The practical significance of the results is that the study can reveal the problems of design and development of educational programs on information security and formulate recommendations for the design.

Keywords: information security, personnel potential, higher school teachers, educational program.

References

1. *Podvedeny itogi plenuma regional'nogo otdeleniya fumo po informatsionnoi bezopasnosti* [The results of the Plenum of the Regional Branch of the Information Security FUMO are summarized], available at: <https://sibsutis.ru/news/3701575/> (accessed 05.07.2022).
2. Ziva S. V., Zakharov D. I. Printsipy postroeniya i opyt realizatsii uchebnogo kursa "Prikladnye voprosy informatsionnoi bezopasnosti" [Principles of construction and experience in the implementation of the training course "Applied issues of information security"]. *Sovremennye informatsionnye tekhnologii i IT-obrazovanie*, 2020, vol.16, no. 4, pp. 980-989. DOI 10.25559/SITITO.16.202004.980-989.
3. Sukhomlin V. A., Belyakova O. S., Klimina A. S., Polyanskaya M. S., Rusanov A. A. Model' tsifrovyykh navykov kiberbezopasnosti 2020 [Model of digital cybersecurity skills 2020]. *Sovremennye informatsionnye tekhnologii i IT-obrazovanie*, 2020, vol.16, no. 3, pp. 695-710. DOI 10.25559/SITO.16.202003.695-710.
4. Avdeeva E. S., Mironova V. V. Formirovaniye grupp strategicheskikh professii kak odin iz instrumentov dostizheniya strategicheskoi konkurentosposobnosti predpriyatii [Formation of groups of strategic professions as one of the tools for achieving the strategic competitiveness of enterprises]. *Izvestiya YUGo-Zapadnogo gosudarstvennogo universiteta. Seriya: EHkonomika. Sotsiologiya. Menedzhment*, 2017, vol. 7, no. 2(23), pp. 148-160.
5. Tsatskina E. P., Lyakhova E. G., Moroz N. Y. O lingvisticheskoi podgotovke kadrov po informatsionnoi bezopasnosti na etape perekhoda k tsifrovoi ekonomike [On linguistic training in information security at the stage of transition to digital economy]. *Obzor pedagogicheskikh issledovaniy*, 2021, no. 3(6), pp. 162-167.

6. Sukhomlin V. A., Belyakova O. S., Klimina A. S., Polyanskaya M. S., Zubareva E. V., Yakushin A. V. *Arkhitektura i printsiipy razrabotki kurrikuluma dlya distsipliny «Kiberbezopasnost'»* [Architecture and principles of curriculum development for the discipline of «Cybersecurity»]. *Sovremennye informatsionnye tekhnologii i IT-obrazovanie*, 2020, no. 16(4), pp. 927-939. DOI 10.25559/SITITO.16.202004.927-939
7. Drozhzhinov V. I. SFIA-sistema professional'nykh standartov v sfere IT epokhi tsifrovoi ekonomiki [SFIA-system of professional standards in IT in the era of digital economy]. *Sovremennye informatsionnye tekhnologii i IT-obrazovanie*, 2017, no. 13(1), pp. 132-143.
8. Tsvetkova O. N. Informatsionnaya bezopasnost' v usloviyakh tsifrovoi ekonomiki v Rossii [Information security in the conditions of digital economy in Russia]. *Samoupravlenie*, 2021, no. 5(127), pp. 440-443.
9. Malyuk A. A., Polyanskaya O. Yu. *Kommentarii k Doktrine informatsionnoy bezopasnosti Rossijskoj Federatsii* [Comments to the Doctrine of Information Security of the Russian Federation]. Moscow: Nauchno-tehnicheskoe izdatel'stvo "Goryachaya liniya-Telekom", 2018, 102 p. ISBN 978-5-9912-0711-9.
10. Malyuk A. A., Polyanskaya O. Yu. *Etika v sfere informatsionnykh tekhnologii* [Ethics in the sphere of information technologies]. *Vestnik Rossijskogo humanitarnogo nauchnogo fonda*, 2011, no. 4(65), pp. 72-77.
11. A.Yu. Sogomonov, M.V. Bogdanov *Professional'naya etika inzhenera* [Professional Ethics of Engineer]. Ed. V.I. Bakshtanovsky. Tyumen, Nauchno-issledovatel'skii institut politicheskoi ekonomiki Tyumenskogo issledovatel'skogo universiteta, 2018. 246 p.
12. Olifirov A. V., Makoveichuk K. A., Petrenko S. A. Improving the courses of educational programs on information security smart grid. *CEUR Workshop Proceedings*, 4, Yalta, Crimea, 16-21 September, 2019, Yalta, Crimea, 2021, pp. 340-350.
13. Malyuk A. A., Malyuk Z. P. Aktual'nye voprosy sozdaniya sistemy massovogo obucheniya kul'ture informatsionnoi bezopasnosti [Actual issues of creating a system of mass training culture of information security]. *Bezopasnost' informatsionnykh tekhnologij*, 2021, vol. 28, no.4, pp. 6-21. DOI 10.26583/bit.2021.4.01
14. Bushuyev A. L., Derevtsova I. V., Maltseva Yu. A., Terentyeva V. D. Rol' informatsionnoi bezopasnosti v usloviyakh tsifrovoi ekonomiki [The Role of Information Security in the Digital Economy]. *Baikal Research Journal*, 2020, no. 11(1), pp. 6-6. DOI 10.17150/2411-6262.20.11(1).6.
15. Pilipenko V. V., Kuznetsova M. A. Analiz rossijskogo rynka informatsionnoi bezopasnosti v kontekste razvitiya tsifrovoi ekonomiki [Analysis of the Russian information security market in the context of digital economy development]. *Innovatsionnaya ehkonomika*, 2019, no. 3(20), pp. 4-12.
16. Antonova N.L., Babikova I.I. Informatsionnaya bezopasnost' v usloviyakh tsifrovoi ekonomiki [Information Security in the Digital Economy]. *Zametki uchenogo*, 2020, no. 13, pp. 111-117.
17. Strukova E. G., Mikidenko N. L., Storozheva S. P. Vzaimodeistvie s rabotodatelem kak instrument formirovaniya obrazovatel'noi programmy [Interaction with employer as a tool for educational program formation]. *Informatsionnaya bezopasnost' tsifrovoi ekonomiki XVII nauchno-teoreticheskaja konferentsiya VIII Plenuma regional'nogo otdeleniya Federal'nogo uchebno-metodicheskogo ob"edineniya v sisteme vysshego obrazovaniya po ukрупnennoi gruppe spetsial'nostei i napravlenii podgotovki 10.00.00 "Informatsionnaya bezopasnost'" po Sibirskomu i Dal'nevostochnomu federal'nyy okrugam (SibROUMO)*, Novosibirsk, Sibirskii gosudarstvennyi universitet telekommunikatsii i informatiki, 13–15 October, 2021, pp. 78-94.
18. *Cybersecurity: information protection as a business growth driver*, available at: [Cyber security: information protection as a business growth driver \(megafon.ru\)](https://megafon.ru) (accessed 05.07.2022).
19. *Khabarovsk hosts information security forum "Siberia Far East-2022" 30.06.2022*, available at: <https://minobr.khabkrai.ru/events/Novosti/3606> (accessed 05.07.2022).
20. Batanov A., Brylyakova M. From digitalization to accreditation revolution. Report from parliamentary hearings in State Duma Committee on Education and Science. April, 2022. Website: Accreditation in Education. available at: <https://akvobr.ru/new/publications/273> (accessed 05.07.2022).
21. *Uroki-stress-testa: rossijskie vuzy v usloviyakh pandemii i posle nee* [Analytical Report "Stress-Test Lessons: Russian Universities in Pandemic and Post-Pandemic Conditions"] June, 2020. available at: [003_Доклад.pdf \(yandex.ru\)](https://yandex.ru) (accessed 05.07.2022).