УДК 372.8, 004.056
DOI 10.54835/18102883_2023_34_6

РАЗРАБОТКА МОДЕЛИ АКТУАЛИЗАЦИИ ПРОФЕССИОНАЛЬНЫХ КОМПЕТЕНТНОСТЕЙ СПЕЦИАЛИСТА ПО КИБЕРБЕЗОПАСНОСТИ В УСЛОВИЯХ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

Сизов Валерий Александрович,
доктор технических наук, профессор, профессор кафедры прикладной информатики и информационной безопасности,
Sizov.VA@rea.ru

Киров Алексей Дмитриевич,
ассистент кафедры прикладной информатики и информационной безопасности,
Kirov.AD@rea.ru

Российский экономический университет им. Г.В. Плеханова,
Высшая школа кибертехнологий, математики и статистики,
Россия, 117997, г. Москва, Стремянный пер., 36

Ландшафт угроз кибербезопасности в последнее время стал значительно более разнообразным в силу повышения интенсивности информационного противоборства в экономической, политической и военной сферах. Современная ситуация в условиях цифровой трансформации экономики России требует от системы подготовки специалистов по кибербезопасности учета динамики развития тактик и техник проведения нарушителями кибербезопасности атак на субъекты экономической деятельности, а также соответствующих способов и инструментальных средств противодействия этим атакам. Работа посвящена разработке модели формирования профессионально-технических компетентностей специалиста по кибербезопасности, учитывающей теорию и практику развития методов, инструментальных средств и форм информационного противоборства. В ней представлен подход описания противоборства на основе теории графов, предложен способ оценки уровня квалификации специалиста по кибербезопасности в зависимости от его способности противодействовать нарушителям кибербезопасности. Целью работы является разработка модели актуализации профессионально-технических компетентностей специалиста по кибербезопасности в условиях информационного противоборства, позволяющей определять актуальный набор этих компетентностей для достижения требуемого уровня кибербезопасности субъекта экономической деятельности. Разработанная модель использует статистическое распределение Рэлея и учитывает соотношение уровня квалификации специалиста по кибербезопасности и нарушителя кибербезопасности. Она позволяет исследовать динамику уровня обеспечения кибербезопасности субъекта экономической деятельности в зависимости от конкретного соотношения уровня квалификации специалиста по кибербезопасности и нарушителя кибербезопасности. Представленные в работе результаты компьютерного эксперимента свидетельствуют об их адекватности реальности.

Ключевые слова: Информационное противоборство, кибербезопасность, подготовка профессиональных кадров, компетентность специалиста по кибербезопасности, моделирование, графы, эффективность.

Цифровая трансформация экономики России охватывает все большие экономические сферы и проникает практически во все ее структурные компоненты, включая кадровое обеспечение. Широкое использование информационных технологий, развитие киберпространства быстро меняют экономический ландшафт и требуют комплексного решения задач обеспечения информационной безопасности субъектов экономической деятельности (СЭД) в условиях усиления киберугроз, распространения практики применения методов и средств информационного противоборства.

Глобальные расходы на решения по кибербезопасности увеличиваются. По прогнозам Gartner, в целом расходы на кибербезопасность в мире достигнут $188,3 млрд в 2023 г., а к 2026 г. превысят $260 млрд. Центр стратегических разработок утверждает, что в ближайшие 5 лет отечественный рынок кибербезопасности предположительно вырастет со 185,9 до 469 млрд р. [1, 2].

Быстрое развитие разнообразных отечественных и зарубежных способов и средств защиты киберпространства предъявляет особые требования к профессиональным компетентностям инженера (специалиста по кибер-

безопасности), при формировании которых необходимо учитывать множество факторов, включая возможности и действия злоумышленников в условиях информационного противоборства. При этом у СЭД обостряется конкурентная борьба за высококвалифицированные кадры в сфере кибербезопасности, что делает проблему подготовки этих кадров значимой в масштабе экономики страны.

Современная ситуация требует от системы подготовки специалистов по кибербезопасности не только реализации цели формирования их ключевых компетентностей (универсальных способов действия) [3, 4], но также формирования профессионально-технических компетентностей, учитывающих теорию и практику развития методов, инструментальных средств и форм информационного противоборства.

Сложность задачи формирования специальных компетентностей специалистов по кибербезопасности определяется необходимостью их периодической актуализации на основе данных мониторинга кибербезопасности в условиях информационного противоборства [5–8].

Многие компании на базе HRM-платформ разрабатывают цифровые профили персонала, включающие профессиональные компетентности, которые позволяют компании увязать свои глобальные цели с индивидуальными целями работников, помогают стимулировать развитие их профессиональных знаний, умений, навыков [6, 9].

Разработка и применение цифровых профилей персонала в инженерно-технической области позволяет более качественно оценивать степень соответствия специальных компетентностей работника должному уровню осуществления его профессиональной деятельности, а также определять способность работника к адекватной оценке собственного профессионального уровня и умение проектировать свое развитие как инженера. Причем при подготовке инженерных кадров большое значение имеет фактор содержания специальных компетентностей, его актуальность с технологической точки зрения в условиях цифровой трансформации экономики.

Кроме этого, в условиях информационного противоборства в киберпространстве инженерные кадры, отвечающие за допустимый уровень кибербезопасности СЭД должны обладать способностью противодействовать нарушителям кибербезопасности, использующим современные тактики и техники проведения атак в информационном пространстве СЭД.

Проблеме формирования компетентностей специалистов по кибербезопасности в зарубежной печати посвящено множество публикаций. Среди них выделяются статьи, в которых представлен обзор литературы по развитию компетентностей в области кибербезопасности, как в профессиональной сфере [10, 11], так и в высшем образовании [12, 13]. Авторы этих работ анализируют существующие подходы к определению компетентностей, а также выделяют ключевые компетентности, необходимые для успешной работы в данной профессиональной области. В работе [12] предлагаются рекомендации для улучшения программ обучения кибербезопасности в высшем образовании и развития компетентностей у студентов. При этом вопросы, связанные с подготовкой кадров высшей квалификации, которым предстоит осуществление профессиональной деятельности в условиях информационного противоборства в киберпространстве, напрямую не рассматриваются. В работе [13] представлены различные подходы к обучению кибербезопасности, а также анализируются вызовы, связанные с разработкой и реализацией программ обучения в данной области, например, определения компетентностей в области кибербезопасности для персонала в условиях удаленной работы. Другие работы предлагают определенные наборы компетентностей в области кибербезопасности для рабочей силы [14–17], для медицинских работников [18], для профессионалов в области промышленного управления системами [19], для правоохранительных органов [20] и др. В этих работах предлагаются методы оценки уровня компетентностей в области кибербезопасности работников соответствующих субъектов экономической деятельности. Однако эти методы комплексно не учитывают развитие средств защиты и нападения в современном киберпространстве, а также дифференцированные уровни компетентностей нарушителей кибербезопасности и специалистов по кибербезопасности, которые призваны защищать информационное пространство СЭД от действующих атак и будущих возможных атак в киберпространстве.

Анализ научных и методических источников и результаты поисково-аналитического эксперимента позволили выявить противо-

речие актуализации содержания компетентностей специалиста по кибербезопасности в системе повышения квалификации: между возрастающими требованиями государства и бизнеса к специальным компетентностям специалиста по кибербезопасности в условиях информационного противоборства и недостаточной разработанностью педагогических условий их актуализации в системе повышения квалификации.

Поэтому научная задача разработки модели актуализации профессиональных компетентностей специалиста по кибербезопасности в условиях информационного противоборства представляется очень важной. Целью решения данной задачи является формирование формализованного инструмента актуализации матрицы компетентностей специалиста по кибербезопасности для своевременной адаптации образовательных программ к изменяющимся условиям развития информационного противоборства, включая развитие тактик и техник атак, проводимых нарушителями кибербезопасности, а также способов и инструментальных средств защиты от них.

Задача представляет собой определение характера и степени зависимости уровня кибербезопасности СЭД от времени и соотношения уровня квалификации специалиста по кибербезопасности к уровню квалификации нарушителя кибербезопасности. Решение данной задачи позволяет выявить условия, при которых уровень обеспечения кибербезопасности СЭД будет допустимым. При этом уровень квалификации специалиста по кибербезопасности и нарушителя кибербезопасности полностью определяется соответствующими наборами компетентностей. Это упрощение в данном случае допустимо, поскольку в условиях информационного противоборства в каждой атаке можно выделить, с одной стороны, тактики и техники, используемые нарушителем кибербезопасности, и, с другой стороны, определить необходимые способы и инструментальные средства, которые специалист по кибербезопасности должен уметь использовать для противодействия злоумышленнику. Таким образом непротиворечиво реализуется принцип «действие–противодействие».

В качестве исходных данных для определения уровня квалификации противоборствующих сторон целесообразно использовать графовые методы анализа.

Пусть A – множество трудовых действий специалиста по кибербезопасности $A=\{a_1,a_2,a_3,\ldots a_n\}$; B – множество техник, используемых нарушителями кибербезопасности $B=\{b_1,b_2,b_3,\ldots b_m\}$.

Множество трудовых действий специалиста по кибербезопасности можно определить соответствующими отраслевыми профессиональными стандартами либо задать исходя из требований конкретного СЭД.

Множество техник, используемых нарушителями кибербезопасности, можно определить из открытых источников: базы знаний, разработанной и поддерживаемой в актуальном состоянии корпорацией MITRE на основе анализа реальных атак [21], и ежегодного отчета Агентства Европейского Союза по кибербезопасности ENISA [22].

Каждой технике b_i можно сопоставить одно или несколько трудовых действий a_i из множества A.

Тогда соответствие множеству техник, используемых нарушителями кибербезопасности A, множества трудовых действий специалиста по кибербезопасности B, может быть определено следующим образом:

$$W_{AB} = \|w_{ij}\|, i = \overline{1,n},\ j = \overline{1,m},$$

где W_{AB} – матрица инцидентности графа G_{AB}, представленного на рис. 1,

$$w_{ij} = \begin{cases} 1, \text{ если } i\text{-я техника связана} \\ \text{с } j\text{-м действием специалиста} \\ \text{по кибербезопасности СЭД;} \\ 0 \text{ в противном случае,} \end{cases}$$

n – количество техник, используемых нарушителями кибербезопасности; m – количество трудовых действий специалиста по кибербезопасности.

Для того чтобы подготовка специалистов по кибербезопасности была практикоориентированной, необходимо сформировать компетентности, связанные со способами применения соответствующих инструментальных средств противодействия той или иной технике. Список сертифицированных инструментальных средств (средств защиты информации) представлен на сайте ФСТЭК [23].

Пусть C – множество инструментальных средств противодействия техникам, $C=\{c_1,c_2,c_3,\ldots c_k\}$. В качестве инструментальных средств противодействия известным техникам могут использоваться средства защиты информации, представленные в Государственном реестре сертифицированных средств защиты информации (рис. 2)

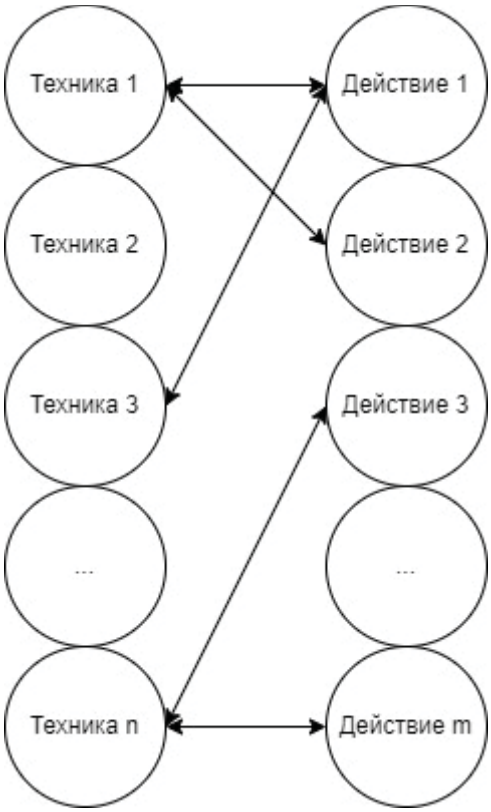

Рис. 1. Граф G_{AB} соответствия техник и трудовых действий

Fig. 1. Graph G_{AB} of correspondence between techniques and labor actions

№ сертификата	Дата внесения в реестр	Срок действия сертификата	Наименование средства (шифр)
17/1	26.07.2002	01.08.2020	фильтр сетевой помехоподавляющий ФСПК-100(200)-0,22/0,38-91 УХЛ4
21/2	25.06.2013	25.06.2019	программный комплекс защиты информации от НСД «Страж 1.1»
27/1	24.05.2005	24.05.2020	устройство «Корунд»
32/1	20.04.1996	17.04.2021	система защиты информации от несанкционированного доступа «Снег 2.0»
32/2	20.04.1996	17.04.2021	система защиты информации от несанкционированного доступа «Снег 2.0»
41/5/10	30.03.2011	30.03.2020	система защиты «Гром-ЗИ-4»
41/5/17	18.04.2013	18.04.2019	система защиты «Гром-ЗИ-4»
41/6/5	09.03.2011	09.03.2020	система защиты «Гром-ЗИ-4А»
41/6/47	30.10.2012	30.10.2018	система защиты «Гром-ЗИ-4А»

Рис. 2. Фрагмент Государственного реестра сертифицированных средств защиты информации

Fig. 2. Fragment of the State Register of Certified Information Security Tools

Тогда с учетом функционального описания этих средств защиты информации можно построить граф соответствия техник нарушителя кибербезопасности трудовым действиям специалиста по кибербезопасности и используемым средствам защиты информации (рис. 3).

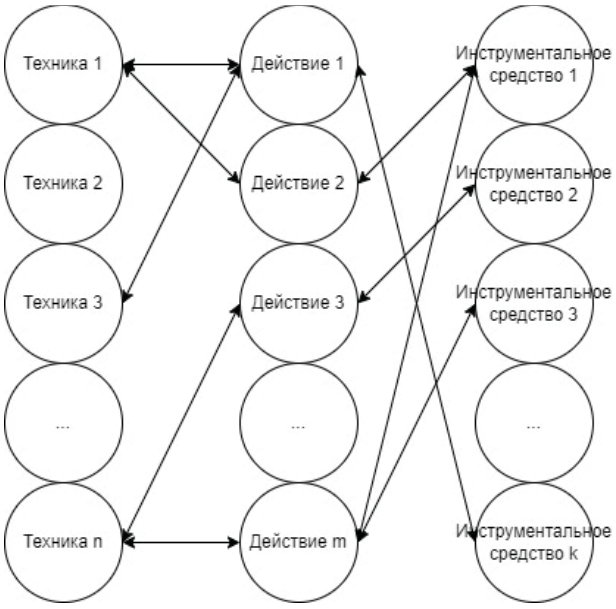

Рис. 3. Граф G_{BC} соответствия техник нарушителя кибербезопасности, трудовых действий специалиста по кибербезопасности и используемых средств защиты информации

Fig. 3. Graph G_{BC} of correspondence between the techniques of a cybersecurity violator, the labor actions of a cybersecurity specialist and the information security tools used

Соответствие множества B трудовых действий специалиста по кибербезопасности множеству C инструментальных средств противодействия техникам может быть определено следующим образом:

$$W_{BC} = \|w_{jl}\|, \; j = \overline{1,m}, l = \overline{1,k},$$

где W_{BC} – матрица инцидентности графа G_{BC} взаимосвязей трудовых действий специалиста по кибербезопасности и инструментальных средств противодействия техникам,

$$w_{jl} = \begin{cases} 1, \text{ если } j\text{-е действие специалиста} \\ \text{по кибербезопасности СЭД} \\ \text{связано с } l\text{-м инструментальным} \\ \text{средством противодействия} \\ \text{техникам;} \\ 0 \text{ в противном случае,} \end{cases}$$

m – количество трудовых действий специалиста по кибербезопасности; k – количество инструментальных средств противодействия техникам.

Функциональное описание средств защиты информации и покрытие этими средствами техник, представленных в матрице MITRE ATT&CK [21], определяется производителями средств киберзащиты, например, на сайте ведущего разработчика решений для информационной безопасности Positive Technologies

представлено покрытие техник этой матрицы различным цветом для конкретного средства защиты информации [24] (рис. 4). В данной модели предполагается, что каждое трудовое действие обеспечено необходимыми инструментальными средствами противодействия, т. е. необеспеченные инструментальными средствами противодействия техникам трудовые действия специалиста по кибербезопасности отсутствуют:

$$\sum_{l=1}^{k} w_{jl} \neq 0, \forall j = \overline{1,m}.$$

Рис. 4. Фрагмент матрицы MITRE ATT&CK для продукта Positive Technologies

Fig. 4. Fragment of the MITER ATT&CK matrix for the Positive Technologies product

Для разработки модели актуализации профессиональных компетентностей специалиста по кибербезопасности в условиях информационного противоборства предлагается использовать статистическое распределение Рэлея [9]. В качестве параметра масштаба распределения Рэлея выступает отношение зависимости уровня обеспечения кибербезопасности СЭД от времени и соотношения уровня квалификации специалиста по кибербезопасности и нарушителя кибербезопасности. В этом случае оценка зависимости уровня обеспечения кибербезопасности СЭД от времени и соотношения уровня квалификации специалиста по кибербезопасности и нарушителя кибербезопасности имеет следующий вид:

$$P(t,\sigma) = \frac{t}{\sigma^2} \times e^{\frac{-t^2}{2\sigma^2}}, t \geq 0, \sigma > 0,$$

где P – уровень обеспечения кибербезопасности СЭД в момент времени t; σ – отношение уровня квалификации специалиста по кибербезопасности к уровню квалификации нарушителя кибербезопасности.

Пусть i-я техника нарушителя кибербезопасности, применяемая в атаке на СЭД, является угрозой кибербезопасности.

Тогда при $\sum_{j=1}^{m} w_{ij} = 0$ эта угроза реализуема, т. к. специалист по кибербезопасности ей не может противодействовать.

Пусть $\sum_{i=1}^{m} x_i$ – уровень таких угроз кибербезопасности, где

$$x_i = \begin{cases} 1, \text{ если } \sum_{j=1}^{m} w_{ij}=0; \\ 0 \text{ в противном случае.} \end{cases}$$

На практике основной задачей специалиста по кибербезопасности является поддержание текущего риска кибербезопасности в допустимых пределах риска кибербезопасности. Тогда в первом приближении должно выполняться требование

$$x_{\min} \leq \sum_{i=1}^{n} x_i \leq x_{\max},$$

где $x_{\min}$ – минимально возможный для конкретного СЭД уровень угроз кибербезопасности; $x_{\max}$ – максимально возможный для конкретного СЭД уровень угроз кибербезопасности.

Тогда соотношение уровня квалификации специалиста по кибербезопасности конкретного СЭД и уровня квалификации нарушителя кибербезопасности, заданное на множестве компетентностей «действие–противодействие», может быть выражено следующим образом:

$$\sigma = \frac{x_{\max} - \sum_{i=1}^{n} x_i}{x_{\max}} = 1 - \frac{\sum_{i=1}^{n} x_i}{x_{\max}}.$$

В случае когда противоборствующие стороны (специалист по кибербезопасности и нарушитель кибербезопасности) – группы людей, к этим группам можно применять групповые количественные оценки уровня их квалификации [6].

Для оценки работоспособности модели актуализации профессиональных компетентностей специалиста по кибербезопасности в условиях информационного противоборства проведен компьютерный эксперимент.

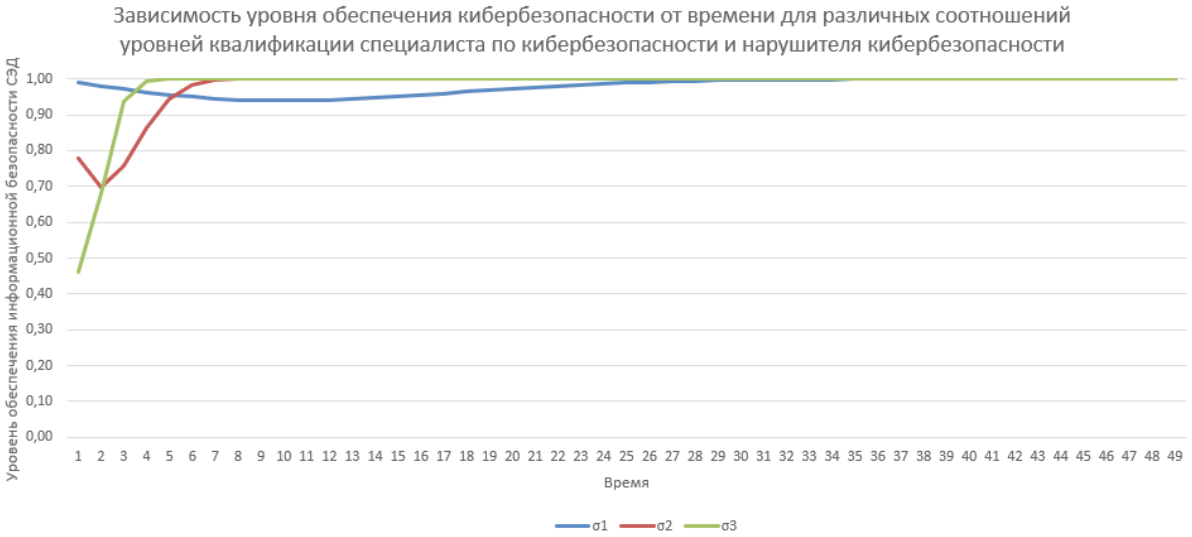

Рис. 5. Графики зависимости уровня обеспечения кибербезопасности СЭД от времени для различных соотношений уровня квалификации специалиста по кибербезопасности конкретного СЭД и уровня квалификации нарушителя кибербезопасности

Fig. 5. Graphs of dependence of EDMS cybersecurity level on time for various ratios of qualification level of a cybersecurity specialist for a particular EDMS and th qualification level of a cybersecurity violator

В качестве исходных данных использовались следующие соотношения уровня квалификации специалиста по кибербезопасности конкретного СЭД и уровня квалификации нарушителя кибербезопасности: σ_1=0,1; σ_2=0,5; σ_3=0,9.

Результаты моделирования представлены на графике (рис. 5).

Анализ представленных на рис. 5 графиков показывает следующее. В случае когда уровень квалификации специалиста по кибербезопасности значительно превышает уровень квалификации нарушителя кибербезопасности (график для σ_3) в ходе проведения злоумышленником атаки на СЭД, уровень обеспечения кибербезопасности СЭД быстро растет до максимального.

В случае когда уровень квалификации нарушителя кибербезопасности значительно превышает уровень квалификации специалиста по кибербезопасности (график для σ_1) в ходе проведения злоумышленником атаки на СЭД, уровень обеспечения кибербезопасности СЭД быстро снижается некоторое время и далее медленно восстанавливается до максимального уровня.

Для случая равных уровней квалификации специалиста по кибербезопасности и нарушителя кибербезопасности (график для σ_2) в ходе проведения злоумышленником атаки на СЭД наблюдается незначительное, но продолжительное снижение уровня обеспечения кибербезопасности СЭД.

Таким образом, использование статистического распределения Рэлея в этой модели адекватно и непротиворечиво отражает динамику эффективности решения задачи обеспечения кибербезопасности СЭД в зависимости от соотношения уровней квалификации специалиста по кибербезопасности и нарушителя кибербезопасности.

Предложенная модель актуализации профессиональных компетентностей специалиста по кибербезопасности может быть использована для разработки и уточнения отраслевых профессиональных стандартов в области кибербезопасности различных СЭД, а также в системе повышения квалификации для определения требуемого уровня актуализации компетентностей специалиста по кибербезопасности в условиях информационного противоборства.

Работа выполнена при финансовой поддержке ФГБОУ ВО «РЭУ им. Г.В. Плеханова».

СПИСОК ЛИТЕРАТУРЫ

1. Кибербезопасность 2022–2023. Тренды и прогнозы. URL: https://www.ptsecurity.com/ru-ru/research/analytics/ogo-kakaya-ib/?utm_source=yandex&utm_medium=cpc&utm_campaign=83387165-search-cyber-keywords&utm_content=5134114004-13515166514&calltouch_tm=yd_c:83387165_

gb:5134114004_ad:13515166514_ph:43371020357_st:search_pt:premium_p:1_s:none_dt:desktop_reg:213_ret:43371020357_apt:none&_openstat=ZGlyZWN0LnlhbmRleC5ydTs4MzM4NzE2NTsxMzUxNTE2NjUxNDt5YW5kZXgucnU6cHJlbWl1bQ&yclid=11017443921774510079#id1 (дата обращения 17.05.2023).
2. Российский рынок кибербезопасности может вырасти в 2,5 раза к 2026 году. URL: https://www.vedomosti.ru/business/news/2022/08/02/934195-rossiiskii-rinok-kiberbezopasnosti-mozhet-virasti (дата обращения 17.05.2023).
3. Андреев А.Л. Компетентностная парадигма в образовании: опыт философско-методологического анализа // Педагогика. – 2005. – № 4. – С. 19–27.
4. Макаренко А.С. Методика воспитательной работы: Избранные труды. – М.: Юрайт, 2020. – 323 с.
5. Сизов В.А., Киров А.Д. Проблемы внедрения SIEM-систем в практику управления информационной безопасностью субъектов экономической деятельности // Открытое образование. – 2020. – Т. 24. – № 1. – С. 69–79. DOI: https://doi.org/10.21686/1818-4243-2020-1-69-79
6. Джинчарадзе Г.Р. Методические аспекты организации процедуры оценки персонала // ИВД. – 2012. – № 2. URL: https://cyberleninka.ru/article/n/metodicheskie-aspekty-organizatsii-protsedury-otsenki-personala (дата обращения: 17.05.2023).
7. Модель цифровых навыков кибербезопасности / В.А. Сухомлин, О.С. Белякова, А.С. Климина, М.С. Полянская, А.А. Русанов. – М.: Фонд Лига интернет-медиа, 2021. – 294 с.
8. Назарова О.Б., Масленникова О.Е., Давлеткиреева Л.З. Формирование компетенций специалиста в области информационных систем с привлечением вендоров // Прикладная информатика. – 2013. – № 2 (44). – С. 49–56.
9. Сизов В.А., Киров А.Д. Разработка моделей аналитической системы обработки данных для мониторинга ИБ объекта информатизации, использующего облачную инфраструктуру // Russian Technological Journal. – 2021. – Т. 9. – № 6 (44). – С. 16–25. DOI: 10.32362/2500-316X-2021-9-6-16-25. EDN GHQHQC.
10. Мамаева А.М. Совершенствование системы внутрифирменного обучения персонала // Молодежь и наука: шаг к успеху. Сборник научных статей 3-й Всероссийской научной конференции перспективных разработок молодых ученых: в 5 т. Т. 1 – Курск: Университетская книга, 2019. – С. 288–291.
11. Нихайчик А.П., Шендель Т.В. Обучение производственного персонала: критерии и показатели результативности // Международный журнал прикладных и фундаментальных исследований. – 2017. – № 2-2. – С. 246–248.
12. Competencies for cybersecurity professionals: a systematic literature review / Yusuf Perwej, Syed Qamar Abbas, Jai Pratap Dixit, Nikhat Akhtar, Anurag Kumar Jaiswal // International Journal of Scientific Research and Management. – 2021. – V. 9. – Iss. 12. – P. 669–710.
13. Bendler D., Felderer M. Competency models for information security and cybersecurity professionals: analysis of existing work and a new model // ACM Transactions on Computing Education. – 2022. – V. 22. – № 4. – P. 1–35. DOI: 10.1145/3573205.
14. Learn to train like you fight / M. Karjalainen, A.-L. Ojala, M. Vatanen, J. Lötjönen // International Journal of Adult Education and Technology. – 2023. – V. 14. – № 1. – P. 1–20. DOI: 10.4018/IJAET.322085.
15. Hijji Mohammad, Alam Gulzar. Cybersecurity Awareness and Training (CAT) framework for remote working employees // Sensors. – 2022. – № 22. – P. 1–18. DOI: 10.3390/s22228663.
16. Wang Ping, D'Cruze Hubert. Certifications in cybersecurity workforce development: a case study // International Journal of Hyperconnectivity and the Internet of Things. – 2019. – № 3. – P. 38–57. DOI: 10.4018/IJHIoT.2019070104.
17. Ghosh Tirthankar, Iii Guillermo. Assessing competencies using scenario-based learning in cybersecurity // Journal of Cybersecurity and Privacy. – 2021. – № 1. – P. 539–552. DOI: 10.3390/jcp1040027.
18. Helser S. Healthcare in the balance: a consequence of cybersecurity // Journal of The Colloquium for Information Systems Security Education. – 2022. – V. 9. – № 1. – P. 1–5. DOI: 10.53735/cisse.v9i1.145.
19. Remote training in cybersecurity for industrial control systems / M. Domínguez, D. Pérez, A. Moran, S. Alonso, M. Prada, J. Fuertes // IFAC-PapersOnLine. – 2022. – V. 55. – № 17. – P. 320–325. DOI: 10.1016/j.ifacol.2022.09.299.
20. A conceptual learning framework of cybersecurity education for military and law enforcement: workforce development / A. Nag, V. Bhadauria, C. Gibson, R Neupane, D. Creider // International Journal of Smart Education and Urban Society. – 2022. – V. 13. – № 1. – P. 1–14. DOI: 10.4018/IJSEUS.309953.
21. MITRE ATT&CK. URL: https://attack.mitre.org/ (дата обращения: 17.05.2023).
22. Отчет об угрозах ENISA за 2022 г. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 (дата обращения: 17.05.2023).
23. Государственный реестр сертифицированных средств защиты информации. URL: https://fstec.ru/en/153-tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/sistema-sertifikatsii/591-gosudarstvennyj-reestr-sszi (дата обращения: 17.05.2023).
24. Какие техники MITRE ATT&CK выявляют продукты Positive Technologies. URL: https://mitre.ptsecurity.com/ru-RU/techniques?utm_source=seclab&utm_medium=news (дата обращения: 17.05.2023).

Поступила: 29.06.2023
Принята: 20.10.2023

UDC 372.8, 004.056
DOI 10.54835/18102883_2023_34_6

DEVELOPMENT OF A MODEL FOR UPDATING PROFESSIONAL COMPETENCES OF A CYBERSECURITY SPECIALIST IN INFORMATION CONFIRMATION

Valirii A. Sizov,
Dr. Sc., Professor,
Sizov.VA@rea.ru

Alexey D. Kirov,
Assistant,
Kirov.AD@rea.ru

Plekhanov Russian University of Economics,
36, Stremyanny lane, Moscow, 117997, Russia

The landscape of cybersecurity threats has recently become much more diverse due to the increase in the intensity of information confrontation in the economic, political and military spheres. The current situation in the context of digital transformation of the Russian economy requires the training system for cybersecurity specialists to take into account the dynamics of development of tactics and techniques for carrying out attacks by violators of cybersecurity on economic entities, as well as appropriate methods and tools to counter these attacks. The work is devoted to development of a model for formation of professional and technical competencies of a cybersecurity specialist, taking into account the theory and practice of developing methods, tools and forms of information confrontation. The paper introduces an approach to describing confrontation based on graph theory, and proposes a method for assessing the level of qualification of a cybersecurity specialist depending on his ability to counter violators of cybersecurity. The aim of the work is to develop a model for updating the professional and technical competencies of a cybersecurity specialist in the context of information confrontation, which allows determining the actual set of these competencies in order to achieve the required level of cybersecurity of an economic entity. The developed model uses the Rayleigh statistical distribution and takes into account the ratio of the skill level of a cybersecurity specialist and a cybersecurity violator. It allows you to explore the dynamics of the level of ensuring the cybersecurity of an economic entity, depending on the specific ratio of the level of qualification of a cybersecurity specialist and a violator of cybersecurity. The results of a computer experiment presented in the paper testify to their adequacy to reality.

Keywords: Information confrontation, cybersecurity, training professional personnel, competence of a cybersecurity specialist, modeling, graphs, efficiency.

The research was financially supported by the Plekhanov Russian University of Economics.

REFERENCES

1. *Kiberbezopasnost 2022–2023. Trendy i prognozy* [Cybersecurity 2022–2023. Trends and Forecasts]. Available at: https://www.ptsecurity.com/ru-ru/research/analytics/ogo-kakaya-ib/?utm_source=yandex&utm_medium=cpc&utm_campaign=83387165-search-cyber-keywords&utm_content=5134114004-13515166514&calltouch_tm=yd_c:83387165_gb:5134114004_ad:13515166514_ph:43371020357_st:search_pt:premium_p:1_s:none_dt:desktop_reg:213_ret:43371020357_apt:none&_openstat=ZGlyZWN0LnlhbmRleC5ydTs4MzM4NzE2NTsxMzUxNTE2NjUxNDt5YW5kZXgucnU6cHJlbWl1bQ&yclid=11017443921774510079#id1 (дата обращения 17.05.2023).
2. *Rossiiskiy rynok kiberbezopasnosti mozhet vyrasti v 2,5 raza k 2026 godu* [The Russian cybersecurity market may grow 2.5 times by 2026]. Available at: https://www.vedomosti.ru/business/news/2022/08/02/934195-rossiiskii-rinok-kiberbezopasnosti-mozhet-virasti (accessed 17 May 2023).
3. Andreev A.L. Kompetentnostnaia paradigma v obrazovanii: opyt filosofsko-metodologicheskogo analiza [Competency paradigm in education: experience of philosophical and methodological analysis]. *Pedagogika*, 2005, no. 4, pp. 19–27.
4. Makarenko A.S. *Metodika vospitatelnoy raboty: Izbrannye Trudy* [Methods of educational work: Selected works]. Moscow, Uright Publ., 2020. 323 p.
5. Sizov V.A., Kirov A.D. Problemy vnedreniia SIEM-sistem v praktiku upravleniya informatsionnoy bezopasnostiyu subektov ekonomicheskoy deiatelnosti [Problems of introducing SIEM systems into the practice of managing information security of subjects of economic activity]. *Otkrytoe obrazovanie*, 2020, vol. 24, no. 1, pp. 69–79.

6. Dzhincharadze G.R. Metodicheskie aspekty organizatsii protsedury otsenki personala [Methodological aspects of the organization of the personnel assessment procedure]. *IVD*, 2012, no. 2. Available at: https://cyberleninka.ru/article/n/metodicheskie-aspekty-organizatsii-protsedury-otsenki-personala (accessed 17 May 2023).
7. Sukhomlin V.A., Beliakova O.S., Klimina A.S., Polianskaia M.S., Rusanov A.A. *Model tsifrovykh navykov kiberbezopasnosti* [Cybersecurity digital skills model]. Moscow, Fond Liga internet-media Publ., 2021. 294 p.
8. Nazarova O.B., Maslennikova O.E., Davletkireeva L.Z. Formirovanie kompetentsii spetsialista v oblasti informatsionnykh sistem s privlecheniem vendorov [Formation of competencies of a specialist in the field of information systems with the involvement of vendors]. *Prikladnaia informatika*, 2013, no. 2 (44), pp. 49–56.
9. Sizov V.A., Kirov A.D. Razrabotka modeley analiticheskoy sistemy obrabotki dannykh dlya monitoringa IB obekta informatizatsii, ispolzuiushchego oblachnuyu infrastrukturu [Development of models of an analytical data processing system for monitoring information security of an informatization object using cloud infrastructure]. *Rossiyskiy tekhnologicheskiy zhurnal*, 2021, vol. 9, no. 6, pp. 16–25. DOI: 10.32362/2500-316X-2021-9-6-16-25.
10. Mamaeva A.M. Sovershenstvovanie sistemy vnutrifirmennogo obucheniia personala [Improving the system of in-company personnel training]. *Molodezh i nauka: shag k uspekhu. Sbornik nauchnykh statey 3-y Vserossiyskoy nauchnoy konferentsii perspektivnykh razrabotok molodykh uchenykh: v 5 t. T. 1* [Youth and science: a step to success. Collection of scientific articles of the 3rd All-Russian scientific conference on promising developments of young scientists: in 5 vol. Vol. 1]. Kursk, Universitetskaya kniga Publ., 2019. pp. 288–291.
11. Nikhaichik A.P., Shendel T.V. Obuchenie proizvodstvennogo personala: kriteriii pokazately rezultativnosti [Training of production personnel: criteria and performance indicators]. *Mezhdunarodny zhurnal prikladnykh i fundamentalnykh issledovanii*, 2017, no. 2-2, pp. 246–248.
12. Yusuf Perwej, Syed Qamar Abbas, Jai Pratap Dixit, Nikhat Akhtar, Anurag Kumar Jaiswal. Competencies for cybersecurity professionals: a systematic literature review. *International Journal of Scientific Research and Management*, 2021, vol. 9, Iss. 12, pp. 669–710.
13. Bendler D., Felderer M. Competency models for information security and cybersecurity professionals: analysis of existing work and a new model. *ACM Transactions on Computing Education*, 2022, vol. 22, no. 4, pp. 1–35. DOI: 10.1145/3573205.
14. Karjalainen M., Ojala A.-L., Vatanen M., Lötjönen J. Learn to train like you fight. *International Journal of Adult Education and Technology*, 2023, vol. 14, no. 1, pp. 1–20. DOI: 10.4018/IJAET.322085.
15. Hijji Mohammad, Alam Gulzar. Cybersecurity Awareness and Training (CAT) framework for remote working employees. *Sensors*, 2022, no. 22, pp. 1–18. DOI: 10.3390/s22228663.
16. Wang Ping, D'Cruze Hubert. Certifications in cybersecurity workforce development: a case study. *International Journal of Hyperconnectivity and the Internet of Things*, 2019, no. 3, pp. 38–57. DOI: 10.4018/IJHIoT.2019070104.
17. Ghosh T., Iii G. Assessing competencies using scenario-based learning in cybersecurity. *Journal of Cybersecurity and Privacy*, 2021, no. 1, pp. 539–552. DOI: 10.3390/jcp1040027.
18. Helser S. Healthcare in the balance: a consequence of cybersecurity. *Journal of The Colloquium for Information Systems Security Education*, 2022, vol. 9, no. 1, pp. 1–5. DOI: 10.53735/cisse.v9i1.145.
19. Domínguez M., Pérez D., Moran A., Alonso S., Prada M., Fuertes J. Remote training in cybersecurity for industrial control systems. *IFAC-PapersOnLine*, 2022, vol. 55, no. 17, pp. 320–325. DOI: 10.1016/j.ifacol.2022.09.299.
20. Nag A., Bhadauria V., Gibson C., Neupane R., Creider D. A Conceptual learning framework of cybersecurity education for military and law enforcement: workforce development. *International Journal of Smart Education and Urban Society*, 2022, vol. 13, no. 1, pp. 1–14. DOI: 10.4018/IJSEUS.309953.
21. *MITRE ATT&CK*. Available at: https://attack.mitre.org/ (accessed: 17 May 2023).
22. *Otchet ob ugrozakh ENISA za 2022 g.* [2022 ENISA Threat Report]. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 (accessed: 17 May 2023).
23. *Gosudarstvenny reestr sertifitsirovannykh sredstv zashchity informatsii* [State register of certified information security tools]. Available at: https://fstec.ru/en/153-tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/sistema-sertifikatsii/591-gosudarstvennyj-reestr-sszi (accessed: 17 May 2023).
24. *Kakie tekhniki MITRE ATT&CK vyyavlyayut produkty Positive Technologies* [Which MITER ATT&CK techniques identify Positive Technologies products]. Available at: https://mitre.ptsecurity.com/ru-RU/techniques?utm_source=seclab&utm_medium=news (accessed: 17 May 2023).

Received: 29.06.2023
Accepted: 20.10.2023