УДК 004.056

С.П. Серёдкин[1]

[1] Иркутский государственный университет путей сообщения, г. Иркутск, Россия

УНИВЕРСИТЕТСКИЙ ЦЕНТР КОМПЕТЕНЦИЙ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, СОВРЕМЕННОЕ ПРЕДСТАВЛЕНИЕ

Аннотация. В данной работе рассматриваются основные подходы к созданию центра компетенций по информационной безопасности. Представлена комплексная модель центра компетенций как структуры, необходимой для управления интеллектуальным капиталом в регионе, на платформе ведущего университета, системы обладающей необходимым потенциалом и способностью к постоянной генерации. Выделены особенности центра компетенций как структуры, нацеленной на активный поиск, трансфер и накопление новых знаний и уникального опыта. Систематизированы задачи, решаемые в рамках центра компетенций и направления его развития. Приведен авторский опыт проектирования университетских центров компетенций.

Ключевые слова: центр компетенций, профессиональные компетенции, инновационные задачи, перманентное образование.

S.P. Seryodkin1

[1]Irkutsk State Transport University, Irkutsk, Russia

Abstract. This paper discusses the main approaches to the creation of an information security competence center. A comprehensive model of the competence center is presented as a structure necessary for managing intellectual capital in the region, on the platform of a leading university, a system with the necessary potential and the ability to continuously generate. The features of the competence center as a structure aimed at active search, transfer and accumulation of new knowledge and unique experience are highlighted. The tasks solved within the competence center and the directions of its development are systematized. The author's experience in designing university competence centers is given.

Keywords: competence center, professional competencies, innovative tasks, permanent education.

Введение. Проблемы, связанные с обеспечением безопасности информации в информационных инфраструктурах Российской Федерации, в настоящее время приобрели новую значимость. Начиная с февраля 2022 года, мировое информационной пространство становится плацдармом для ведения информационных войн, целью которых является повышение общей эффективности вооруженных сил путем повсеместного внедрения военных информационных функций таких как психологические операции, электронная война, дезинформация и прямые информационные атаки. Сложность и критичность создавшейся ситуации подтверждается аналитическими данными об многократном увеличении количества кибератак на информационную инфраструктуру государства. Обеспечение информационной безопасности Российской Федерации является ключевой задачей государства по обеспечению национальной безопасности при условии повышения уровня информационной безопасности граждан, общества и государства.

Проблематика. Одной из серьёзных проблем обеспечения информационной безопасности государственных органов это наличие подготовленных кадров [2]. Современный рынок труда выдвигает новые требования к выпускникам, в свою очередь очевидным является тот факт, что уровень подготовки выпускников вузов не удовлетворяет ожиданиям работодателей. По данным опроса предприятий и организаций по заказу газеты «Ведомости», уровнем знаний выпускников вузов недовольны более половины отечественных работодателей [2]. У работодателей изменились требования к молодым специалистам, им нужен подготовленный специалист с опытом работы. На первый взгляд можно сказать, что это завышенные требования ведь молодежь не имеет возможности получить опыт работы и одновременно междисциплинарную специальность, обучаясь в вузе. Но и у работодателей по объективным причинам нет времени на практическое обучение, так как в современных условиях беспрецедентного возрастающего уровня киберугроз они должны обеспечить

надежность функционирования информационной инфраструктуры. Острота и критичность данного аспекта подтверждает тот факт, что Президентом и Правительством РФ в период с 2022 по 2024 год принимается ряд важных документов по повышению уровня информационной безопасности. Наиболее значимые из них: 1. «Указ Президента Российской Федерации от 01.05.2022 № 250» [4] нацелен на повышения уровня информационной безопасности критической информационной инфраструктуры и определяет требования к созданию подразделений по информационной безопасности; 2.«Постановление Правительства РФ от 15 июля 2022 г. N 1272» [5] определяет требования к квалификации ответственного лица за обеспечение информационной безопасности в субъекте критической информационной инфраструктуры, а также знаний, умений и профессиональных компетенций.

Данные государственные решения направлены на повышение уровня защиты ключевой информационной инфраструктуры Российской Федерации. Требования вышеуказанных государственных инициатив направленны на повышение механизма ответственности подразделений и персонала субъектов КИИ по обнаружению, предупреждению и ликвидации последствий компьютерных атак, и реагированию на компьютерные инциденты. В конечном счете высоким требованиям к квалификации и уровню подготовки выпускников вузов по направлению «информационная безопасность» и на преодоление разрыва в ожиданиях требования работодателей и квалификаций выпускников.

Парадигма исследования. Актуальность и своевременность необходимости мер направленных на повышение уровня подготовки и квалификации специалистов по ИБ подтверждает тот факт, что по поручению Президента Российской Федерации В.В.Путина, реализуется проект по созданию центра компетенций, инициатором выступает президентская платформа «Россия — страна возможностей» при поддержке Министерства науки и высшего образования Российской Федерации [6]. Как показывает практика необходимость проекта по созданию ЦКИБ в настоящее время продиктовано требованием государства и жизненной необходимостью.

Следует отметить, что центр компетенций необходимо рассматривать как структуру обеспечивающую процесс перманентного высокопрофессионального образования, которая способна решать следующие задачи:

- консультирование и экспертные заключения по вопросам, требующим междисциплинарного подхода в профессиональной деятельности;
- выработка новых решений в соответствие с контекстом внешней среды, современными тенденциями и технологическим развитием;
- формирование новых идей, способствующее внедрению инноваций;
- развитие партнерских взаимоотношений между университетами;
- содействие созданию корпоративных образовательных структур, корпоративно-инновационных центров;
- совершенствование материально-технического обеспечения учебных дисциплин и развитие информационной инфраструктуры;
- сбор, применение, развитие имеющихся и создание новых корпоративные знаний.

В связи с активизацией инновационных процессов за последнее десятилетие в России сформировалось несколько типов центров компетенций. Можно выделить следующие основные типы:

1. Корпоративные. Такие центры компетенций создаются в рамках отдельной компании и направлены на решение ее инновационных задач. Корпоративные центры компетенций, как правило, сфокусированы на оптимизацию бизнес-процессов, их методическое обеспечение, разработку стандартов производственной деятельности и обучение персонала [7].

2. Университетские. Создаются для партнерского сотрудничества университета с академической наукой (РАН) — для совместного выполнения прорывных фундаментальных исследований и их доведения до внедрения инноваций в народном хозяйстве.

3. Отраслевые. Функционируют в отдельных отраслях экономики и сформированы для решения определенных задач. Зачастую могут выполнять функцию мульти дисциплинарной платформы для развития научных знаний в разных направлениях отраслевой исследовательской деятельности.

4. Региональные. Данные центры компетенций в основном организованы в виде партнерства науки (университетов) и бизнеса, обеспечивают передачу знаний от науки к бизнесу для решения прорывных задач территорий.

Центр компетенций – это структура, нацеленная на поиск новых знаний, их активный трансфер и оказание консультационных, сервисных и высокопрофессиональных услуг. Конкурентоспособность центра компетенций определяется первоклассным уровнем и креативностью сотрудников, их мотивацией к саморазвитию и наращиванию интеллектуального капитала [8].

Подходы к проектированию. Цель проекта: 1. Оценить и развить универсальные компетенции у студентов адаптировать их к потребностям рынка;

2. Повысить уровень профессиональных умений и знаний у специалистов по ИБ предприятий через процесс интеграции в систему дополнительного образования.

Реализация этих целей позволит создать механизм перманентного образования как в университетской среде, так и на предприятиях региона. в свою очередь компетентностный профиль откроет обучающимся доступ к подходящим вакансиям, стажировкам, проектам и возможностям дальнейшего профессионального роста.

Главной задачей ЦКИБ на наш взгляд является подготовка студентов с востребованным уровнем знаний к профессиональным компетенциям, совершенствование «надпрофессиональных» компетенций преподавателей, повышение квалификации специалистов по ИБ учреждений и организаций региона. Для решения этих задач необходимо в содружестве вуза и работодателя гибко реагировать на изменения требований рынка к уровню подготовки специалистов по ИБ.

По мнению автора, в основу проектирования центра компетенций должны быть положены следующие основные принципы: концептуальность; распределенное лидерство; управление на основе базовых ценностей; взаимодействие и партнерские отношения с инновационным бизнесом. На основании результатов анализа теоретических, методических и практических аспектов были сформированы предложения для организационно-функциональной модели центра компетенций на платформе ведущего университета рис.1.

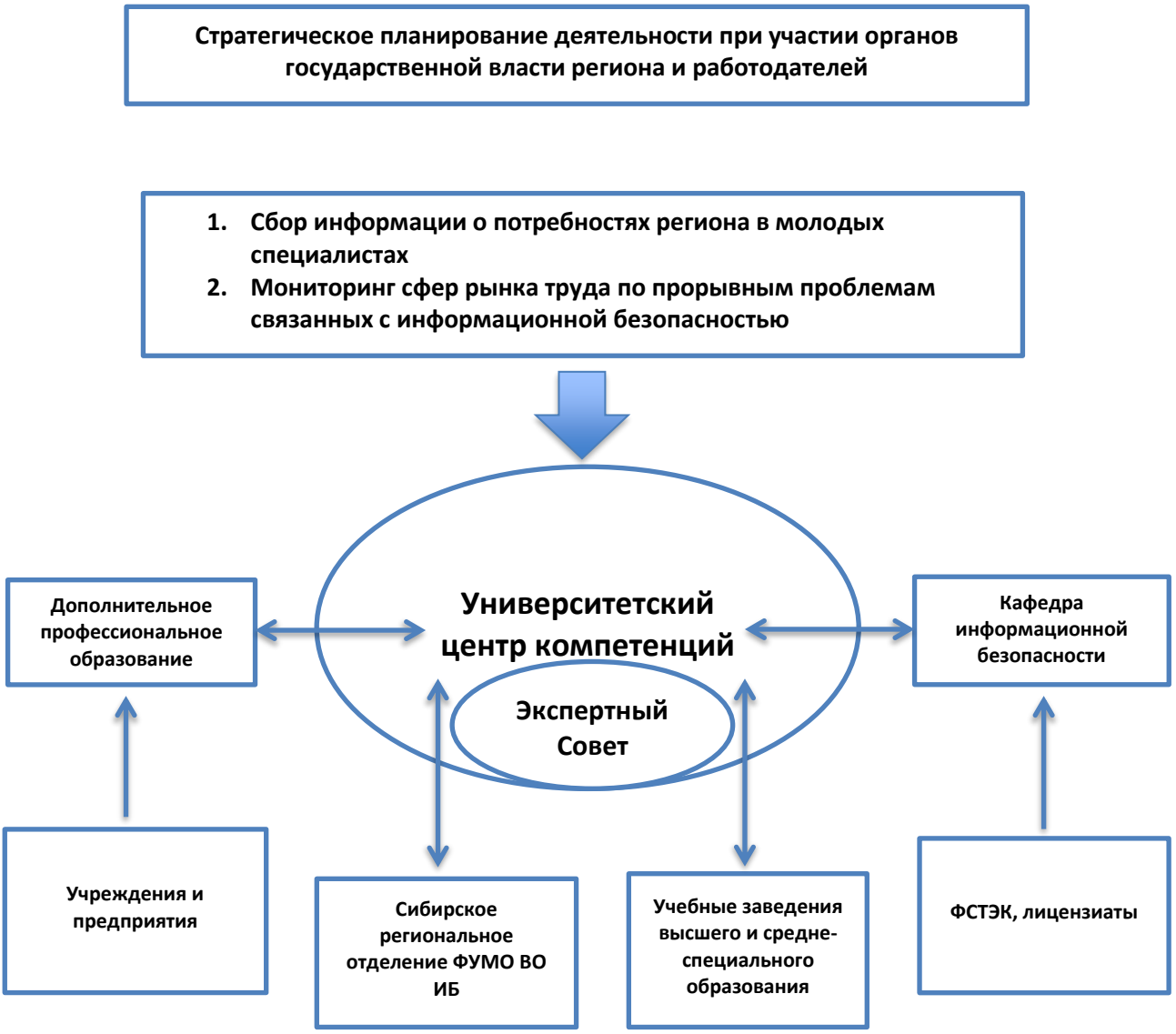

Рис. 1. Организационно-функциональная модель центра компетенций

Модель регионального центра компетенций по информационной безопасности на платформе ведущего университета представляет собой специально выделенную структуру, основной целью которой является активизация деятельности в части формирования новых знаний и компетенций, популяризация основного и дополнительного образования, для удовлетворения потребностей региона в специалистах по защите информации.

Как структура высокопрофессиональных услуг ЦКИБ призван решать следующие задачи:

- развитие и укрепление нормативно-правовой и организационно-технической базы информационной безопасности;
- выявление и формализация неявных знаний предприятий работодателей;
- сбор, систематизация и распространение внутрикорпоративных знаний;
- консультирование и экспертные заключения по вопросам, требующим междисциплинарного подхода и поиска новых знаний в образовании;

- выработка новых решений в методологическом обеспечении образовательного процесса в соответствие с требованием внешней среды, глобальными тенденциями и прогрессивными технологиями;
- обеспечение непрерывных контактов между работодателями и центром компетенций по вопросам генерации, привлечения, трансляции и расширения интеллектуального капитала, информация о котором сосредоточена в центре;
- формирование системы развития талантов, как основы для расширения интеллектуального капитала региона, в первую очередь, человеческого капитала;
- организация акселерационных программ для авторов и руководителей проектов, направленных на преумножение интеллектуального капитала региона;
- генерация новых идей, способствующая внедрению инноваций в вопросах информационной безопасности;
- формирование и развитие информационной инфраструктуры поддержки деятельности ЦКИБ, включающей региональную базу знаний, а также данных систематизированной и регулярно обновляемой информации о наличии предложений вузов и «горячих» вакансиях работодателей.

При создании ЦКИБ необходимо учитывать возможные трудности:

- недостаток молодых перспективных специалистов, а вместе с этим энтузиазма, свежих идей, готовности к постоянному развитию;
- возможная высокая стоимость информационного обеспечения;
- загруженность экспертов текущей работой и нехватка времени на сбор и обмен знаниями;
- проблемы старения профессорско-преподавательского состава, отток преподавателей наиболее перспективного группы 35-45 лет, недостаточный уровень компетентности преподавателей вузов.

По нашему мнению, для создания ЦКИБ на базе ведущего университета необходимо задействовать потенциалы кафедр и системы дополнительного образования, с привлечением к диалогу ключевых работодателей региона. Для совершенствования универсальных компетенций студентов необходима экспертиза со стороны лицензиатов ФСТЭК в части доработки рабочих программ дисциплин и требований к оснащению учебных лабораторий.

Заключение. Какие результаты дает проект создания ЦКИБ:

Университету – обеспечить выпуск молодых специалистов, максимально адаптированных к задачам современного рынка труда.

Студенту – получить возможность к реализации эффективного социального и карьерного роста. Центр компетенций даст возможность оценить студентам свои навыки и сформировать индивидуальную траекторию их развития. На основе результатов диагностики и прохождения траектории сформировать профиль студента, доступный работодателям. Это откроет обучающемуся доступ к подходящим вакансиям, стажировкам и проектам.

Работодателю – возможность привлечь молодые кадры с требуемыми компетенциями. Работодатели получают доступ к базе студентов и недавних выпускников, прошедших диагностики валидными и надежными инструментами оценки, а также сумевших развить имеющиеся навыки и подчеркнуть свои сильные стороны.

Региону - деятельность Центра компетенций позволит сохранять и повышать качество человеческого ресурса, не отпуская молодые кадры за пределы территории, а предлагая максимально востребованные позиции и возможности для карьерного и социального развития в регионе. Повышать профессиональный уровень специалистов по информационной безопасности учреждений и предприятий на основе реализации программ повышения квалификации и профессиональной переподготовки.

Таким образом, представленная модель может быть реализована для обеспечения целей концентрации, координации, трансляции и генерации интеллектуального капитала в регионе и обеспечить необходимые предпосылки для её эффективного использования на рынке.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Указ Президента РФ от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации».
2. В Минцифры рассказали о проблемах подготовки кадров по информбезопасности в регионах. – URL: https://infoforum.ru/glavnoe/v-mincifry-rasskazali-o-problemah-podgotovki-kadrov-po-informbezopasnosti-v-regionah (дата обращения: 17.04.2024).
3. Уровнем знаний выпускников вузов недовольны более половины отечественных работодателей. - URL: https://www.superjob.ru/community/life/59162/?from_refresh=1 (дата обращения: 17.04.2024).
4. Указ Президента РФ от 01.05.2022 N 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации". – URL: https://www.consultant.ru/document/cons_doc_LAW_416198 (дата обращения: 17.04.2024).
5. Постановление Правительства Российской Федерации от 15.07.2022 № 1272 "Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)". – URL: http://static.government.ru/media/acts/files/1202207190035.pdf (дата обращения: 17.04.2024).
6. Центры компетенций. – URL: https://rsv.ru/competitions/project/1/f9d73c66-a75b-4f01-bc37-287165289a9c/ (дата обращения: 17.04.2024).
7. Гительман Л.Д., Исаев А.П., Кожевников М.В., Гаврилова Т.Б. ИННОВАЦИОННЫЕ МЕНЕДЖЕРЫ ДЛЯ ТЕХНОЛОГИЧЕСКОГО СУВЕРЕНИТЕТА СТРАНЫ. Стратегические решения и риск-менеджмент. 2023;14(2):118-135.
8. Мальцева, А.А. (2020) Основы формирования центров компетенций как структур управления интеллектуальным капиталом на региональном уровне. Вестник ТвГУ. Серия: Экономика и управление (1). С. 52-59. ISSN 2219-1453
9. Искусственный интеллект, импортозамещение, дефицит кадров и другие технотренды 2024 года. – URL: https://rg.ru/2024/01/07/iskusstvennyj-intellekt-importozameshchenie-deficit-kadrov-i-drugie-tehnotrendy-2024-goda.html (дата обращения: 17.04.2024).
10. Гительман Л. Д., Кожевников М. В. Парадигма управленческого образования для технологического прорыва в экономике // Экономика региона. — 2018. — Т. 14, вып. 2. — С. 433–449
11. Менеджеры прорыва. Востребованы амбициозные идеи и лидеры / Л.Д. Гительман, А.П. Исаев. – М.: Инфра-М, 2015. – 152 с. - ISBN 978-5-16-011724-9. – URL: https://bookmix.ru/book.phtml?id=2238924&ysclid=ltvaldvrf823756146 (дата обращения: 17.04.2024).
12. Фабрики знаний: как новый мир перевернул высшее образование/ - URL: https://info.sibnet.ru/article/579433/?ysclid=ltvar8rczv475168213 (дата обращения: 17.04.2024).
13. В российской информационной безопасности кадровая катастрофа. – URL: https://www.cnews.ru/news/top/2021-12-07_v_rossii_kadrovaya_katastrofa?ysclid (дата обращения: 17.04.2024).
14. Кадры в ИБ. Новые вызовы. – URL: https://cisoclub.ru/kadry_v_ib/?ysclid=ltvaxmr (дата обращения: 17.04.2024).

15. В 28 регионах центры компетенций работают неэффективно Об этом сообщает "Рамблер". – URL: https://news.rambler.ru/other/43054404-v-28-regionah-tsentry-kompetentsiy-rabotayut-neeffektivno/ (дата обращения: 17.04.2024).

REFERENCES

1. Decree of the President of the Russian Federation No. 400 dated July 2, 2021 "On the National Security Strategy of the Russian Federation".
2. The Ministry of Finance spoke about the problems of training information security personnel in the regions. – URL: https://infoforum.ru/glavnoe/v-mincifry-rasskazali-o-problemah-podgotovki-kadrov-po-informbezopasnosti-v-regionah (17.04.2024).
3. More than half of domestic employers are dissatisfied with the level of knowledge of university graduates. - URL: https://www.superjob.ru/community/life/59162/?from_refresh=1 (17.04.2024).
4. Decree of the President of the Russian Federation dated 05/01/2022 No. 250 "On additional measures to ensure information security of the Russian Federation". – URL: https://www.consultant.ru/document/cons_doc_LAW_416198 (17.04.2024).
5. Resolution of the Government of the Russian Federation dated 07/15/2022 No. 1272 "On approval of the model Regulation on the deputy head of the body (organization) responsible for ensuring information security in the body (organization) and the model regulation on the structural unit in the body (organization) ensuring information security of the body (organization)". – URL: http://static.government.ru/media/acts/files/1202207190035.pdf (17.04.2024).
6. Competence Centers. – URL: https://rsv.ru/competitions/project/1/f9d73c66-a75b-4f01-bc37-287165289a9c/ (17.04.2024).
7. Gitelman L.D., Isaev A.P., Kozhevnikov M.V., Gavrilova T.B. INNOVATION MANAGERS FOR THE COUNTRY'S TECHNOLOGICAL SOVEREIGNTY. Strategic decisions and risk management. 2023;14(2):118-135.
8. Bases of competence centers formation as intellectual capital management structures. At the regional level. A.A. Maltseva. Lurye Scientific and Methodological Center for Higher School Innovative Activity of Tver State University, Tver. 58. P. 52-59. ISSN 2219-1453
9. Artificial intelligence, import substitution, shortage of personnel and other technological trends in 2024. – URL: https://rg.ru/2024/01/07/iskusstvennyj-intellekt-importozameshchenie-deficit-kadrov-i-drugie-tehnotrendy-2024-goda.html (17.04.2024).
10. Gitelman, L. D. & Kozhevnikov, M. V. (2018). A Paradigm of Managerial Education for a Technological Breakthrough in the Economy. Ekonomika regiona [Economy of Region], 14(2), 433–449
11. Breakthrough managers. Ambitious ideas and leaders are in demand / L.D. Gitelman, A.P. Isaev. – M.: Infra-M, 2015. – 152 c. - ISBN 978-5-16-011724-9. – URL: https://bookmix.ru/book.phtml?id=2238924&ysclid=ltvaldvrf823756146 (17.04.2024).
12. Knowledge Factories: How the new world turned higher education around / - URL: https://info.sibnet.ru/article/579433/?ysclid=ltvar8rczv475168213 (17.04.2024).
13. There is a personnel disaster in Russian information security. – URL: https://www.cnews.ru/news/top/2021-12-07_v_rossii_kadrovaya_katastrofa?ysclid (17.04.2024).
14. Personnel in the IB. New challenges. – URL: https://cisoclub.ru/kadry_v_ib/?ysclid=ltvaxmr (17.04.2024).
15. In 28 regions, competence centers operate inefficiently. This is reported by Rambler. – URL: https://news.rambler.ru/other/43054404-v-28-regionah-tsentry-kompetentsiy-rabotayut-neeffektivno/ (17.04.2024).

Информация об авторе

Сергей Петрович Серёдкин – к.э.н., доцент кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: sseryodkin2008@yandex.ru.

Author

Sergei Petrovich Seryodkin – Ph. D. in Economics, Associate Professor, the Subdepartment of Information systems and information security, Irkutsk State Transport University, Irkutsk, e-mail: sseryodkin2008@yandex.ru.

Для цитирования

Серёдкин С.П. Современный взгляд на толкование понятия кибербезопасность // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. – 2024. – №1. – С.45-52. – Режим доступа: http://ismm-irgups.ru/toma/121-2024, свободный. – Загл. с экрана. – Яз. рус., англ. (дата обращения: 17.04.2024)

For citations

Seryodkin S.P. Modern view on the interpretation of the concept of cybersecurity // Informacionnye tehnologii i matematicheskoe modelirovanie v upravlenii slozhnymi sistemami: elektronnyj nauchnyj zhurnal [Information technology and mathematical modeling in the management of complex systems: electronic scientific journal], 2024. No. 1. P. 45-52. [Accessed 17/04/24]