

УДК 316

СПЕЦИФИКА КАРЬЕРНОГО РАЗВИТИЯ ПРИ ПЕРЕХОДЕ К ИНФОРМАЦИОННОЙ ЦИВИЛИЗАЦИИ

Чукаев К.Е.

магистрант,

Сочинский государственный университет,

Сочи, Россия

Салова Т.Л.

кандидат технических наук, доцент,

кафедра Информационных технологий и математики,

Сочинский государственный университет,

Сочи, Россия

Аннотация

В статье исследуются особенности карьерного развития в процессе перехода к информационной цивилизации. Показано, как цифровые технологии влияют на профессиональные навыки и карьерные пути. В условиях растущего спроса на специалистов в области информационных технологий, подчеркивается важность таких твердых навыков, как программирование, облачные технологии и анализ данных, а также, таких мягких навыков, как аналитическое мышление и коммуникабельность. Делается вывод, что для успешной адаптации к изменениям на рынке труда в условиях быстро развивающейся цифровой экономики, необходимо постоянное обучение и переобучение, что открывает новые возможности для профессионалов и способствует их успешной карьере в будущем.

Ключевые слова: информационные технологии, информационная цивилизация, карьерное развитие, цифровые технологии, профессиональные навыки.

THE SPECIFICS OF CAREER DEVELOPMENT IN THE TRANSITION TO INFORMATION CIVILIZATION

Chukaev K.E.

undergraduate,

Sochi State University,

Sochi, Russia

Salova T.L.

candidate of Technical Sciences, an associate professor,

Department of Information Technologies and Mathematics,

Sochi State University,

Sochi, Russia

Annotation

The article examines the features of career development in the process of transition to information civilization. It shows how digital technologies affect professional skills and career paths. With the growing demand for information technology professionals, the importance of hard skills such as programming, cloud technology and data analysis, as well as soft skills such as analytical thinking and communication skills, is emphasized. It is concluded that in order to successfully adapt to changes in the labor market in a rapidly developing digital economy, continuous training and retraining are necessary, which opens up new opportunities for professionals and contributes to their successful careers in the future.

Keywords: information technology, information civilization, career development, digital technologies, professional skills.

Переход к информационной цивилизации, характеризующийся стремительным развитием технологий и увеличением зависимости от цифровых систем, существенно меняет ландшафт карьерного развития во многих отраслях

[3]. Открываются новые возможности для профессионалов, стремящихся построить успешную карьеру в современном мире. В статье рассматривается специфика карьерного развития в информационную эпоху, подчеркиваются необходимые навыки, карьерные траектории и перспективы профессий в этом контексте.

С увеличением использования технологий и цифровых систем, растет спрос на специалистов, способных эффективно работать в этих условиях. Компании различных отраслей активно ищут квалифицированных специалистов для поддержки и развития своих цифровых инфраструктур [8]. Это включает в себя не только ИТ-сферу, но и различные другие отрасли, где технологии играют критическую роль. Например, внедрение автоматизированных систем (ERP, CRM, SCADA) и информатизация государственных учреждений создают новые области применения информационных технологий, что приводит к росту числа вакансий в этих областях.

Для успешной карьеры в информационную эпоху необходимы как твердые, так и мягкие навыки.

Твердые навыки - это конкретные профессиональные знания и умения, необходимые для выполнения определенной работы или решения конкретной задачи. К их числу можно отнести, например, следующие:

– знание современных языков программирования, в частности, таких как Python, C++, Java. Эти навыки необходимы для разработки и поддержки цифровых систем [2, 9];

– облачные технологии и знание принципов работы с такими облачными платформами, как AWS, Azure или Google Cloud. Эти знания необходимы для организации эффективной защиты данных, внедрения средств контроля доступа в облачных средах и оценки облачной безопасности;

– владение технологией анализа Big Data, т.е. умение работать с большими данными, включая анализ, визуализацию и интерпретацию данных. Недаром современное время называют эпохой больших данных и аналитики.

Мягкие навыки – это персональные качества человека, способствующие эффективной работе в коллективе. К ним можно отнести следующие:

– аналитическое мышление, включающее аналитический склад ума, внимание к деталям, усидчивость и способность быстро учиться. Эти навыки необходимы для эффективного анализа проблем и разработки стратегий решения [7];

– коммуникабельность, т.е. умение работать в команде, навыки коммуникации и способность самостоятельно принимать решения. Это важно для координации действий со смежными отделами и заинтересованными сторонами [5].

– лидерство и критическое мышление, которые рассматриваются как способность руководить командами, критически мыслить и решать сложные проблемы. Эти навыки необходимы для карьерного роста и успеха в динамичной цифровой среде.

Для реализации деятельности в рамках развивающейся цифровой экономики, специалистам необходимо получение соответствующего образования и сертификации, подтверждающей компетентность, которая соответствует современным требованиям работодателей. Соответствие профессиональным стандартам может включать базовые компетенции и специализированные.

Базовые знания по ИТ, компьютерным наукам и смежным направлениям [8]. Это могут быть курсы по программированию, сетевым технологиям, криптографии или управлению безопасностью. Высшее образование не всегда обязательно, но релевантный опыт и кейсы играют решающую роль в карьерном развитии.

Специализированное образование, сертификаты и опыт работы для более высоких должностей. Сертификации, такие как CompTIA Security+, CISSP, и СЕН высоко ценятся в индустрии. В России ожидается появление специальностей, связанных с информационной безопасностью, в значительном числе вузов.

CompTIA Security+ — это глобальная сертификация, которая подтверждает базовые навыки, необходимые для выполнения основных функций безопасности и начала карьеры в области информационной безопасности. Эта сертификация является первой, которую должен получить любой специалист по кибербезопасности, так как она закладывает основы необходимых знаний для различных ролей в этой области. Экзамен включает практические задания, которые помогают оценить способность кандидата решать реальные проблемы в сфере безопасности. Для успешного прохождения экзамена рекомендуется иметь два года опыта работы в IT с акцентом на безопасность или аналогичное обучение. Сертификация CompTIA Security+ также признана Министерством обороны США как базовая сертификация для специалистов по информационной безопасности.

CISSP — это продвинутая сертификация в области информационной безопасности, предлагаемая (ISC)². Она предназначена для опытных специалистов, работающих в области управления безопасностью информации. CISSP охватывает широкий спектр тем, включая архитектуру безопасности, управление рисками, защиту активов и реагирование на инциденты. Основные требования для получения CISSP включают наличие как минимум пяти лет опыта работы в двух или более из восьми доменов знаний CISSP. Эта сертификация высоко ценится работодателями и часто требуется для руководящих позиций в области информационной безопасности.

СЕН — это сертификация, которая подтверждает навыки этичного хакера. Она обучает методам тестирования на проникновение и выявления уязвимостей

систем. Кандидаты изучают техники взлома, которые могут быть использованы для защиты систем от злонамеренных атак. Для получения СЕН требуется знание основ сетевой безопасности и опыт работы в IT. Эта сертификация полезна для тех, кто хочет работать в области кибербезопасности с акцентом на тестирование на проникновение и защиту систем от атак.

Эти три сертификации представляют собой важные шаги для специалистов по кибербезопасности на разных этапах их карьеры. Каждая из них имеет свои уникальные требования и охватывает различные аспекты безопасности информации. Постоянное обучение является одним из главных факторов в карьерном развитии, поскольку технологии быстро меняются и требуют постоянной адаптации.

Карьерные возможности при переходе к информационной цивилизации разнообразны и динамичны.

Карьера часто начинается с роли администратора систем или аналитика, где специалист набирается опыта и развивает свои навыки. Администратор систем занимается внедрением, настройкой и обслуживанием систем, включая обеспечение непрерывности функционирования и контроль за выполнением процедур резервного копирования. Это роль, которая требует базовых компетенций в системном администрировании и начальных знаний в области IT [6, 7].

Следующим шагом развития карьеры может стать переход на роль аналитика, эксперта или архитектора. Эти роли включают более сложные и интересные задачи, такие как анализ угроз, разработка стратегий защиты и проектирование систем безопасности. Аналитики и эксперты могут работать в различных направлениях, включая SOC (Security Operations Center) и DevSecOps.

SOC — это специализированное подразделение, отвечающее за мониторинг и защиту информационных систем организации. DevSecOps — это

подход, который интегрирует безопасность на всех этапах разработки программного обеспечения.

Менеджер и консультант руководят командами и проектами, разрабатывают стратегии, управляют программами и обеспечивают соответствие требованиям. Консультанты предоставляют экспертные услуги и рекомендации клиентам, проводят аудит безопасности и помогают клиентам в реализации мер безопасности. Эти роли требуют сильных лидерских и коммуникативных навыков, а также способности критически мыслить и решать сложные проблемы.

Рынок труда информационного общества характеризуется несколькими ключевыми особенностями: цифровизацией и автоматизацией, развитием дистанционной занятости, глобализацией, изменением формата взаимодействия через онлайн-платформы, ростом значимости IT-специалистов и необходимостью постоянного обучения для адаптации к новым технологиям.

Задачи специалиста зависят от зрелости процессов в компании. На средних предприятиях за кибербезопасность может отвечать системный администратор, который совмещает несколько ролей. На крупных предприятиях за информационную безопасность отвечают целые подразделения и функционируют собственные SOC с внутренним распределением ролей.

Кибербезопасность активно трансформируется в процессе своего развития, специализации превращаются в отдельные карьерные треки. На стыке нескольких направлений возникают новые профессии, например, появляется потребность в аналитиках SOC со знанием машинного обучения [6, 7].

С увеличением числа технологических инноваций и усилением требований к цифровым решениям, спрос на специалистов продолжает расти [1]. Компании всех размеров и отраслей ищут квалифицированных специалистов для поддержки и развития своих цифровых инфраструктур. Это связано с ростом количества угроз и необходимостью защиты информации, что делает сферу

информационной безопасности одной из самых быстрорастущих ветвей в ИТ-индустрии.

Специалисты, особенно с опытом и сертификациями, могут рассчитывать на высокую заработную плату. Уровень заработной платы зависит от опыта, квалификации и региона, но в целом профессии в цифровой экономике являются одними из наиболее высокооплачиваемых. Например, специалисты по информационной безопасности могут рассчитывать на более благоприятные условия, чем программисты или менеджеры по продажам, трудящиеся в других областях ИТ.

Профессии в сфере ИТ позволяют работать в различных странах и компаниях, предоставляя возможность реализации международной карьеры. Многие компании предлагают удаленную работу, что позволяет работать из любой точки мира. Это особенно актуально для специалистов по информационной безопасности [3], которые могут работать с клиентами из разных регионов и стран.

Карьерная траектория в современной цифровой экономике требует дальнейшего исследования и постоянного совершенствования навыков [9, 10].

Карьера часто начинается с роли администратора систем или аналитика, где специалист приобретает опыт и развивает свои навыки. Это роль, которая требует базовых компетенций в системном администрировании и начальных знаний в области ИТ. Администратор систем занимается внедрением, настройкой и обслуживанием систем, включая обеспечение непрерывности функционирования и контроль за выполнением процедур резервного копирования.

Следующим шагом развития карьеры может стать переход в роль аналитика, эксперта или архитектора. Эти роли включают более сложные задачи, такие как анализ угроз, разработка стратегий защиты и проектирование систем

безопасности. Аналитики и эксперты могут работать в различных направлениях, включая SOC и DevSecOps.

В отдельный трек можно выделить преподавателей кибербезопасности. У нас более 120 учебных заведений, которые выпускают специалистов по информационной безопасности. Профессии в этой сфере обеспечивают широкие возможности для карьерного роста и профессионального развития. С увеличением числа технологических инноваций и усилением требований к цифровым решениям, делает эти профессии привлекательными для тех, кто ищет стабильную и интересную карьеру [3].

Цифровизация не только требует новых навыков и знаний, но и имеет множество положительных последствий. Например, переход к новым формам занятости, таким как удаленная работа и гибридная работа, позволяют работникам более эффективно использовать свое время. Кроме того, цифровизация совершенствует цифровую и аналитическую поддержку процессов принятия решений и позволяет:

- повышать производительность и эффективность работы;
- улучшать качество жизни и здоровье работников;
- повышать доступность и качество образования и здравоохранения;
- улучшать условия труда и социальную защиту работников.

Информационное общество не только меняет характер производства, но и уклад жизни. Система ценностей меняется, возрастает значимость культурного досуга по отношению к материальным ценностям. Лица с ограниченными физическими возможностями, в частности, пожилые люди, могут продолжать работать даже после ухода на пенсию, поскольку повышается планка работоспособного возраста.

Хотя информатизация в основном несёт положительные последствия, есть и некоторые отрицательные аспекты. Например, проблема манипулирования сознанием людей через средства массовой информации, снижение значимости

традиционных культурных ценностей за счет навязываемой массовой культуры. Однако, в целом, информатизация является прогрессивным развитием общества, которое обеспечивает человеку достойное место в нем [4, 5].

Адаптация к технологическим изменениям является ключевым фактором карьерного развития в информационном обществе. Специалисты должны быть готовы к постоянному обучению и обновлению своих навыков, поскольку технологии быстро меняются. Участие в тренингах, семинарах и онлайн-курсах, а также получение сертификатов и дополнительной квалификации, являются необходимыми шагами для поддержания своей конкурентоспособности на рынке труда. Это делает профессии в цифровой экономике не только востребованными, но и динамичными и перспективными.

Библиографический список

1. Андреева О. А. Психология в карьерном консультировании: Учебное пособие. - М: Просвещение, 2020. 240 с.
2. Баранов А. Н. Современные тенденции карьерного развития. - СПб: Питер, 2019. 192 с.
3. Волкова И. И. Карьерный рост в условиях цифровизации. - Казань: Институт инновационных технологий, 2021. 155 с.
4. Громько Н. В. Основы карьерного планирования. - М: Аспект Пресс, 2018. 120 с.
5. Ершова Т. С. Информационная культура и карьера: вызовы современности. - Екатеринбург: УрФУ, 2022. 185 с.
6. Зиновьева Н. В. Карьерные стратегии в цифровую эпоху. - Новосибирск: Сибирское университетское издательство, 2020. 210 с.
7. Кузнецова С. П. Молодежь и карьерное развитие. - Москва: Издательство МГУ, 2021. 180 с.

8. Лебедев А. А. Коммуникации в процессе карьерного роста. - Саратов: Научное издание, 2019. 150 с.
9. Масленников В. И. Профессиональная подготовка и карьера. – Ростов н/Д: Феникс, 2022. 200 с.
10. Николаев П. Ф. Адаптация к информационному обществу. - Воронеж: ВГТУ, 2020. 175 с.

Оригинальность 84%