Образование в информационном обществе

СОВРЕМЕННЫЕ ВЫЗОВЫ СИСТЕМЕ ПОДГОТОВКИ КАДРОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Статья рекомендована к публикации членом редакционного совета А. А. Стрельцовым 19.09.2024.

Царегородцев Анатолий Валерьевич

Доктор технических наук, профессор
Российский университет дружбы народов имени Патриса Лумумбы», директор центра разработки и сопровождения информационно-технологических решений
Москва, Российская Федерация
tsaregorodtsev_av@pfur.ru

Малюк Анатолий Александрович

Кандидат технических наук, профессор
Национальный исследовательский ядерный университет «МИФИ», профессор
Москва, Российская Федерация
aamalyuk@yandex.ru

Волков Сергей Дмитриевич

Федеральное государственное автономное образовательное учреждение высшего образования «Российский университет дружбы народов имени Патриса Лумумбы», заместитель директора центра разработки и сопровождения информационно-технологических решений
Москва, Российская Федерация
volkov_sd@pfur.ru

Аннотация

В статье исследуется влияние процессов цифровизации и цифровой трансформации на общество и устанавливается связь этого влияния с процессами обеспечения информационной безопасности. Определяются современные вызовы системе подготовки кадров в области информационной безопасности, анализируется потребность в квалифицированных специалистах как самой сферы информационной безопасности, так и экономики Российской Федерации в целом. Предлагается несколько подходов к повышению качества подготовки специалистов по информационной безопасности, а также подход к внедрению этого процесса в систему среднего профессионального, высшего и послевузовского образования.

Ключевые слова

цифровизация; экономика данных; информационная безопасность; подготовка кадров; универсальные компетенции; высшее образование; дополнительное профессиональное образование

Введение

В современных условиях развития информационного общества в России наблюдается беспрецедентная трансформация технологических устоев общества. Она характеризуется существенным ростом количества коммуникационных каналов, цифровизацией как производственных процессов, так и повседневной жизни. В этот процесс вносят вклад в том числе мероприятия, реализуемые в рамках национальных проектов Российской Федерации, таких как «Цифровая экономика» и, продолжившему его, «Экономика данных». Например, еще несколько лет назад для поступления в университет абитуриенту требовалось лично приехать в город, где этот университет находится, и подать необходимые документы на бумажном носителе в приемную комиссию. Возможной альтернативой была отправка документов почтой, однако это накладывало

https://doi.org/10.52605/16059921_2025_02_119

дополнительные временные затраты и риски на процесс подачи документов. Сегодня же для подачи документов при поступлении в университет достаточно воспользоваться сервисом «Поступление в вуз онлайн» на платформе «Госуслуги», который предоставляет возможность полностью электронной подачи документов и дальнейшего поступления. Другим примером развития цифровых технологий в нашей стране является процесс трудоустройства: с 2021 года, с внедрением новой электронной системы учёта трудовой деятельности работников, продолжение ведения бумажных трудовых книжек стало необязательным (по желанию работника), а при трудоустройстве без опыта работы, с 2022 года работнику сразу заводится электронная трудовая книжка [1]. Также стоит отметить и запущенный совсем недавно Минцифры сервис «Электронные водительские права», позволяющий предъявлять, при необходимости, водительское удостоверение в электронной форме.

Таким образом, процессы цифровизации и цифровой трансформации в настоящее время затрагивают не только отдельные группы людей, но и все общество в целом, проникая даже в самые отдаленные субъекты и регионы нашей страны. При этом очевидно, что техническая реализация этих процессов не может быть обеспечена без увеличения объема вычислительных и серверных мощностей. Стоит обратить внимание, что по данным материалов аналитической компании iKS-Consulting, объем рынка центров обработки данных (ЦОД) в России по итогам 2023 году вырос на 25% по сравнению с предыдущим годом. При этом общее количество стойко-мест в российских ЦОД к концу 2023 года достигло 70,1 тыс. штук, увеличившись на 20,9% в сравнении с годом ранее (рис. 1) [2]. Однако следует отметить, что в такой значительный рост вносят вклад не только процессы перехода на цифровые сервисы, ежегодный рост объемов хранимых и обрабатываемых данных, и увеличение потребности в облачных сервисах, но и уход из России зарубежных компаний на фоне сложившейся геополитической обстановки, внедрение технологий искусственного интеллекта и растущая потребность в высокопроизводительных вычислениях.

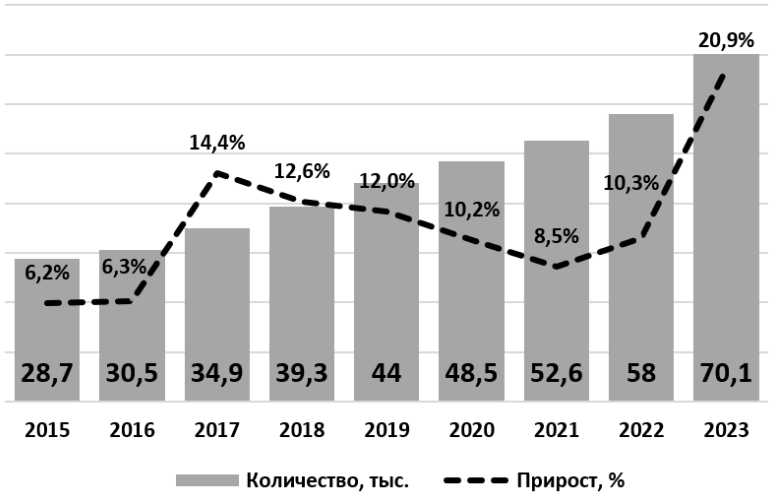

Рис. 1. Динамика роста количества стойко-мест в российских ЦОД в период 2015-2023 гг.

Эта тенденция влечет как положительные, так и отрицательные изменения для общества. В число положительных изменений можно включить: расширение спектра услуг и более широкий доступ к ним за счет повышения доступности, эффективности и скорости их предоставления, расширение доступа к информации и создание новых коммуникационных каналов, и как следствие, возможностей для получения знаний, развитие инноваций и стимулирование технологического прогресса и экономического роста страны. Совокупность отрицательных изменений создает два больших вызова для нашей страны: первый связан с дефицитом квалифицированных кадров в сфере обеспечения информационной безопасности, а второй с уровнем образованности населения в сфере информационной безопасности.

Сопутствующие вызовы создает и рост числа преступлений в цифровой среде, а в свете текущей геополитической обстановки и рост числа политически мотивированных кибератак, а также инцидентов, связанных с фишингом и телефонным мошенничеством. Так, по данным отчета компании F.A.C.C.T. (ранее Group-IB), в 2023 году количество таких атак выросло на 116% по

сравнению с прошлым годом, а целями этих атак были в том числе госучреждения, организации, связанные с критической информационной инфраструктурой, предприятия ОПК [3].

О качестве кадрового обеспечения отрасли информационной безопасности

На фоне всего этого стоит обратить внимание на уже несколько лет привлекающую повышенное внимание проблему кадрового обеспечения отрасли информационной безопасности. Сегодня особенно остро стоит вопрос о повышении численности квалифицированных специалистов в области информационной безопасности, которого невозможно достичь без непрерывного совершенствования образовательного процесса, поскольку теория и практика защиты информационных ресурсов непрерывно и интенсивно развиваются. При этом не только государственные учреждения, но и бизнес-сектор (в т. ч. малый и средний бизнес) выдвигают особые требования к таким специалистам, потому что производственная деятельность будь то государственного учреждения или коммерческой компании все больше опирается на процессы сбора, обработки и анализа информации. По результатам исследования компании Positive Technologies и ЦСР «Северо-Запад» на российском рынке труда в сфере информационной безопасности в 2022–2024 гг. сформировался острый дефицит квалицированных специалистов (рис. 2) [4], а к 2027 году дефицит таких кадров достигнет 60 000 человек [5].

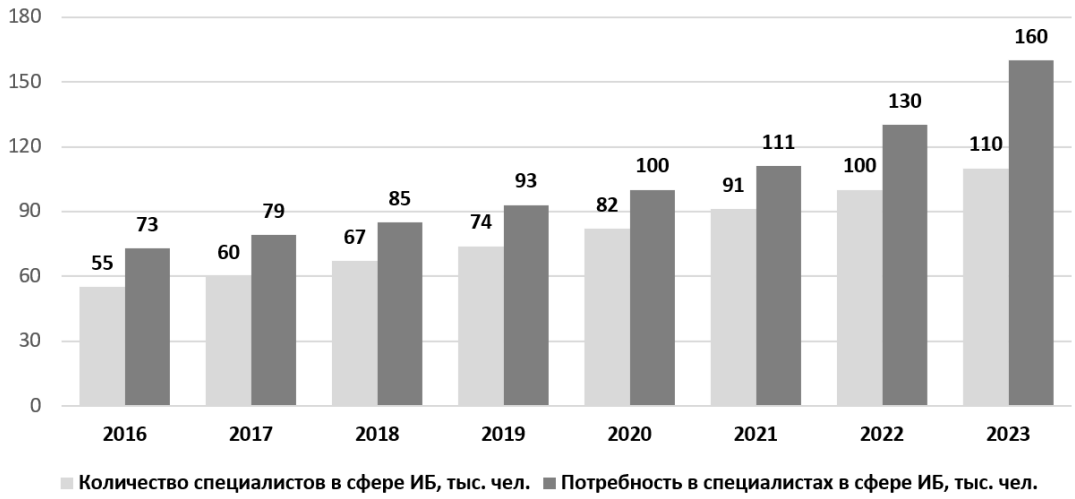

Рис. 2. Динамика роста потребности в квалифицированных специалистах в сфере информационной безопасности

Несмотря на то, что представители Минцифры и представители ФСТЭК, как центра ответственности по УГСНП 10.00.00, сходятся во мнении, что количество выделяемых образовательным организациям бюджетных мест достаточно, чтобы покрыть потребность и государственных органов и бизнес-сообщества в специалистах по информационной безопасности, ситуация с количеством подготовленных квалифицированных специалистов ухудшается из года в год. В этой связи имеет смысл рассмотреть организацию учебного процесса по направлению подготовки «Информационная безопасность» более подробно. Как показывает практика, в большинстве высших учебных заведений, реализующих образовательные программы по УГСНП 10.00.00, содержание дисциплин, преподаваемых в рамках учебных планов, очень сильно отстает от современного развития технологий информационной безопасности. Обратить внимание стоит и на учебные пособия, выпускаемые российскими ВУЗами и рекомендуемыми к использованию в учебном процессе по направлениям подготовки, относящимся к данным УГСНП. Во многих из них рассматриваются программные продукты и технологии 5–10-летней давности, которые в наше время уже не только не поддерживаются производителями, но и морально устарели. При этом, о каких-либо современных аналогах данных продуктов или тенденциях развития в этих трудах не приводится ни слова. В других случаях в учебных пособиях огромная доля внимания уделяется сугубо теоретическим вопросам, которые в практической деятельности будущих специалистов по информационной безопасности никак не встречаются. Например, в рамках дисциплины «Криптографические методы защиты информации» студенты зачастую изучают математические

основы таких алгоритмов как DES, 3DES, ГОСТ 28147–89 (здесь стоит отметить, что новый национальный стандарт шифрования, утвержденный ГОСТ 34.12–2018, в преподавании встречается достаточно редко). При этом за весь курс студентам не показывают ни одного программного или программно-аппаратного средства криптографической защиты информации и тем более не учат с ними работать. Между тем, такая фундаментальная подготовка в области криптографии не потребуется будущему специалисту в практической деятельности, в отличие от навыков работы с криптографическим программным обеспечением и оборудованием: специалист сам не разрабатывает алгоритмы шифрования – он использует те продукты, которые предлагает рынок сертифицированных средств шифрования. В результате получается, что ВУЗ подготовит теоретика, не имеющего никакого представления о том, какие продукты в сфере криптографии существуют на российском рынке и как с ними работать. Конечно, из этого «правила» есть исключения, когда выпускник работает в соответствующих ведомствах или компании-разработчике, однако число таких вакансий несоизмеримо мало в сравнении с потребностью в рядовых специалистах по защите информации. Например, можно взглянуть на статистику наиболее востребованных должностей специалистов сферы информационной безопасности (рис. 3), где видно, что сегодня на рынке труда наиболее востребованы специалисты по защите информации и администраторы средств защиты информации, а потребность, к примеру, в специалистах по криптографической защите информации составляет всего 1% [4].

Рис. 3. Потребность российских организаций в специалистах по защите информации (доля в % от числа вакансий по ИБ)

Продолжая рассмотрение вопроса организации образовательного процесса по информационной безопасности, стоит отметить, что количество университетов, готовящих специалистов по УГСНП 10.00.00 составляет чуть более 140 единиц, при этом лишь треть этих вузов осуществляет подготовку именно квалифицированных специалистов – имеют современную обновляемую материально-техническую базу, квалифицированный профессорско-преподавательский состав, в том числе активно привлекают работников профильных организаций сферы ИБ к реализации образовательного процесса – ведению лекций, проведению практических и лабораторных занятий.

Эксперты сходятся во мнении, что система образования в сфере информационной безопасности должна обеспечивать не только закрытие потребностей сегодняшнего дня, но и быть

направлена на подготовку таких специалистов, кто способен успешно решать перспективные задачи, которые принесёт завтрашний день. Поэтому принимая во внимание и неудовлетворительное состояние материально-технической базы и низкий уровень квалификации профессорско-преподавательского состава в оставшихся двух третьих университетов, остается констатировать тот факт, что они не способны противостоять вызовам цифрового мира.

Для разрешения сложившейся ситуации необходима координация усилий всех участников данных отношений – начиная от самих образовательных организаций, заканчивая бизнес-сообществом и федеральными органами исполнительной власти Российской Федерации. И начать следует в следующих направлениях.

1) Для специальностей и направлений подготовки по 10-й УГСНП ввести целевой прием – либо от организаций, либо от государства, т.е. либо организация платит за обучение таких специалистов, либо государство, а соответственно, по окончании обучения специалист будет обязан отработать несколько лет там, где в нем есть потребность (что позволит планировать, а, главное, гарантировать обеспеченность и потребность всех отраслей и регионов в специалистах по информационной безопасности).

2) Для обеспечения совершенствования материально-технической базы подготовки специалистов по УГСНП 10.00.00 включить в государственное задание тех университетов, где имеется более-менее квалифицированный профессорско-преподавательский состав, статью на обновление и модернизацию их информационной инфраструктуры (за счет экономии средств от прекращения финансирования подготовки по 10-й УГСНП в тех вузах, в которых нет ни материально-технической базы, ни квалифицированного профессорско-преподавательского состава). При этом впоследствии на базе этих университетов станет возможным создание центров коллективного пользования оборудованием с современной постоянно обновляемой материально-технической базой (на базе которых в т.ч. могут создаваться киберполигоны для подготовки специалистов в сфере ИБ), чтобы другие вузы региона могли пользоваться ресурсами такого центра при подготовке своих специалистов, повышая тем самым и их уровень подготовки и квалификацию своих преподавателей.

3) Поскольку основной проблемой при привлечении работников профильных организаций сферы информационной безопасности к реализации образовательного процесса является необходимость их отрыва от основной работы (а с учетом норм учебной нагрузки в университетах, таким работникам приходится проводить чуть ли не большую часть рабочего времени в университетах), целесообразно снизить таким работникам на законодательном уровне нормы учебной нагрузки в среднем до 600 часов в год (из расчета полной ставки), а также освободить их от большинства бюрократических вопросов, связанных с реализацией образовательных программ в высших учебных заведениях по аналогии с решением Минпросвещения России о снижении бюрократической нагрузки на учителей. В результате таких действий и сами профильные организации сферы информационной безопасности будут более активно идти на встречу университетам в части участия их работников в преподавательской работе, и самим работникам не нужно будет «разрываться» между основной работой и университетом [6].

Очевидно, что повышение обеспеченности сферы информационной безопасности высококвалифицированными кадрами не быстрый и трудоемкий процесс, и закрыть такую нехватку кадров «в миг» не удастся. Именно поэтому важнейшим этапом в движении к этой цели является диалог и совместные усилия всех заинтересованных сторон. Одной из основ для начала такого диалога может стать совместная подготовка образовательных стандартов высшего образования будущего поколения (ФГОС 4) с ведущими вендорами и специалистами сферы информационной безопасности. Как показывает статистика (рис. 4), подавляющее большинство специалистов-практиков в сфере информационной безопасности лишь имеют представление об образовательных стандартах, и всего 2% участвовали в их разработке [5].

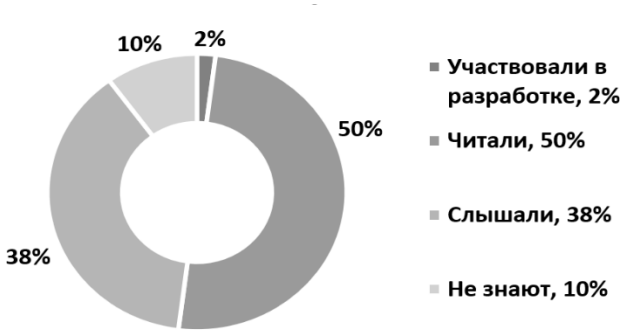

Рис. 4. Степень осведомленности специалистов-практиков об образовательных стандартах в сфере информационной безопасности

На практике это приводит к образованию разрыва между знаниями и умениями, получаемыми в вузах и реальными потребностями рынка. Поэтому такой диалог позволит не только интегрировать опыт ведущих компаний в подготовку будущих специалистов, но и сделать акцент в этой подготовке на изучении тех продуктов и технологий, которые действительно применяются в сфере информационной безопасности сегодня, и с которыми будущему специалисту предстоит взаимодействовать на рабочем месте после получения соответствующего образования.

О подготовке специалистов с компетенциями в области информационной безопасности для экономики данных

Как уже было отмечено, изменения, происходящие в мире под влиянием процессов цифровизации и цифровой трансформации, влияют на все общество в целом, а связь этого влияния с процессами обеспечения информационной безопасности трудно переоценить. Согласно аналитическим материалам российской компании «BI.ZONE» утечка корпоративной почты в среднем происходит у каждого 19-го сотрудника. Эксперты отмечают, что причины утечек чаще всего заключаются в использовании адресов корпоративной почты для регистрации на сторонних сайтах [7]. Кроме того, по данным опросов ВЦИОМ, по итогам 2023 года 67% процентов российских граждан столкнулись со случаями телефонного мошенничества, а само число инцидентов возросло на 70% по сравнению с прошлым годом [8].

В этой связи необходимо отметить важность приобретения компетенций в области информационной безопасности как можно большим числом граждан нашей страны, особенно в свете реализации национального проекта Российской Федерации «Экономика данных». Речь идет о приобретении как технических навыков (hard skills), позволяющих выявлять базовые угрозы безопасности информации (например, с помощью какого программного обеспечения и как определить, являются ли файл или электронное письмо вредоносными, как проверить подлинность веб-сайта и т.д.), так и «мягких» навыков (soft skills), позволяющих, к примеру, оценить правдивость полученной информации, своевременно распознать и предотвратить акт телефонного мошенничества или противодействовать травле в сети Интернет.

Поэтому целесообразным видится встраивание обучения таким навыкам в процесс получения образования – среднего профессионального и высшего – по непрофильным (связанным с ИБ) направлениям подготовки. Рассматривая процесс получения высшего образования, наименее трудозатратным подходом видится включение в федеральные государственные образовательные стандарты всех специальностей и направлений подготовки универсальных компетенций, предусматривающих формирование указанных навыков, а в учебные планы образовательных программ высшего образования соответствующей дисциплины (модуля), например «Основы информационной безопасности в профессиональной деятельности», как это было сделано с модулем «Основы российской государственности» в 2022 году.

Следует также понимать, что высокая скорость процессов цифровизации и цифровой трансформации, появление все более новых технологий и, как следствие, новых угроз, диктуют необходимость создания системы непрерывного образования, направленного на формирование и поддержание компетенций в сфере информационной безопасности. Поэтому этот процесс должен

включать в себя не только обучение определенным аспектам информационной безопасности и защиты информации при подготовке специалистов всех специальностей и направлений подготовки в рамках получения среднего профессионального или высшего образования, но и периодическую актуализацию остаточных знаний работников практически всех отраслей экономики. Данный процесс возможно реализовать в рамках дополнительных образовательных программ, в том числе реализуемых за счет субъектов Российской Федерации в рамках региональных программ, направленных на повышение цифровой грамотности населения, а также в рамках направлений «Кадры» или «Кибербезопасность» национального проекта «Экономика данных».

Центром компетенций в этой задаче мог бы стать межрегиональный учебно-научный центр по мониторингу и исследованию инцидентов кибербезопасности, который совместно с государственными организациями и представителями бизнес-сообщества, заинтересованными в совместной научно-исследовательской, учебно-методической и практической деятельности в области исследования инцидентов информационной и кибербезопасности, будет осуществлять деятельность, направленную на изучение современных методов, средств информационного воздействия и разработке контрмер, направленных на прогнозирование, предупреждение, предотвращение и смягчение последствий от реализации инцидентов информационной и кибербезопасности, а также делиться этим опытом с высшими учебными заведениями, чтобы они могли интегрировать его в качестве «лучших практик» в свои образовательные программы в сфере информационной безопасности.

Межрегиональный учебно-научный центр по мониторингу и исследованию инцидентов кибербезопасности может быть создан под патронажем Министерства науки и высшего образования Российской Федерации с целью вовлечения организаций структуры государственного сектора, профильных отраслевых институтов, регуляторов, органов государственной и исполнительной власти, учреждений высшего образования и прочих заинтересованных сторон, в соответствии со сферой профессиональных интересов, в процесс всестороннего исследования и разработки практических рекомендаций по обеспечению непрерывного мониторинга, выявления и предотвращения инцидентов информационной и кибербезопасности в интересах усиления концепции долгосрочного социально-экономического развития Российской Федерации (рис. 5).

Рис. 5. Высокоуровневая структура организации Межрегионального учебно-научного центра по мониторингу и исследованию инцидентов кибербезопасности

Функционирование Межрегионального учебно-научного центра по мониторингу и исследованию инцидентов кибербезопасности может осуществляться в форме сетевого взаимодействия на правах Консорциума при равноправном партнерстве всех вышеперечисленных участников, а также открытого для вступления других организаций.

Основные задачи Центра по линии учебно-методической деятельности:

1. Разработка методической базы для внедрения в учебный процесс всех специальностей и направлений подготовки дисциплины «Основы информационной безопасности в профессиональной деятельности», интегрирующей междисциплинарные подходы и современные тенденции, направленные на гармонизацию методов решения локальных (отраслевых) задач по обеспечению информационной и кибербезопасности в единую среду обеспечения безопасности и устойчивого развития экономики данных в Российской Федерации.
2. Создание условий для совместного использования учебно-методических и научных наработок, а также материально-технической базы в структуре межрегионального учебно-научного центра по мониторингу и исследованию инцидентов кибербезопасности (в т.ч. на базе центров коллективного пользования оборудованием).
3. Совершенствование материально-технической базы центра: создание универсальной межотраслевой лаборатории по моделированию и исследованию инцидентов информационной и кибербезопасности с возможностью проведения дистанционных исследований и обмена опытом (обучения).
4. Создание и развитие базовых кафедр в области мониторинга и исследования инцидентов информационной и кибербезопасности.

Основные задачи Центра по линии научно-исследовательской деятельности:

1. Участие в разработке и оценке систем нормативных, правовых и методических документов, проведение научных исследований, публикация результатов исследований в сфере мониторинга и расследования инцидентов информационной и кибербезопасности.
2. Развитие и привлечение научного потенциала заинтересованных сторон к непосредственному участию в образовательном процессе, в том числе сотрудников организаций, обладающих знанием и опытом в вопросах управления инцидентами информационной и кибербезопасности.
3. Взаимодействие с отраслевыми высшими учебными заведениями, осуществляющими подготовку кадров и проводящими научные исследования по тематикам деятельности центра.
4. Организация и проведение межрегиональных, всероссийских и международных научно-образовательных мероприятий по тематикам деятельности центра.

Основные задачи Центра по линии совершенствования кадрового потенциала:

1. Реализация программ повышения квалификации населения Российской Федерации в сфере информационной безопасности.
2. Подготовка, переподготовка и повышение квалификации персонала организаций и предприятий в области мониторинга и расследования инцидентов информационной и кибербезопасности.
3. Взаимодействие с отраслевыми высшими учебными заведениями, учебными центрами, центрами профессиональной переподготовки и пр., в целях организации и проведения тренингов и мастер-классов в области мониторинга и расследования инцидентов информационной и кибербезопасности.

Проблемы формирования культуры информационной безопасности

Глобализация информационного пространства ставит перед современным обществом новые вызовы в сфере информационной безопасности, для качественного ответа на которые недостаточно только квалифицированных специалистов в этой области. Руководители, разработчики и простые пользователи современных информационных продуктов должны иметь знания о возможных угрозах информационной безопасности, релевантных для их продуктов, и способах защиты от них; должны понимать свою ответственность и принимать необходимые меры для повышения безопасности этих продуктов. Для решения этих задач в глобальном информационном пространстве необходимо формирование культуры информационной безопасности как части информационной культуры общества.

Необходимость формирования культуры информационной безопасности является не просто современным трендом, а отражает фундаментальные изменения и эволюцию производственных отношений в современном информационном обществе. В декабре 2002 года Генеральная ассамблея ООН приняла резолюцию, в которой были утверждены основные принципы создания глобальной

культуры кибербезопасности, которых должны придерживаться все участники глобального информационного общества [9].

К важнейшим компонентам культуры информационной безопасности можно отнести нормы, правила и стандарты, связанные с обеспечением доверия и безопасности при использовании ИКТ, в том числе рассматривающие и этические нормы их использования.

Одним из ключевых инструментов формирования культуры информационной безопасности в обществе является массовое обучение граждан и интеграция такого обучения в систему непрерывного образования – начиная с дошкольного и кончая послевузовским [11]. Обучение не должно быть ограничено формированием сугубо технических навыков – процесс должен быть построен на формировании понимания важности информационной безопасности и ответственности при использовании ИКТ. Также в процесс обучения должны быть включены занятия, направленные на формирование навыков обнаружения и реагирования на инциденты информационной безопасности, обеспечения непрерывности и восстановления деятельности компьютерных систем, а также навыков компьютерной криминалистики (как обращаться с доказательствами, используемыми при расследовании компьютерных преступлений, и взаимодействовать с правоохранительными органами). Современная практика показывает, что обучение основам информационной безопасности и этики при использовании ИКТ дает существенно больший вклад в укрепление безопасности, чем какие-либо другие меры. Таким образом, обучение нравственности и этике (прежде всего, современной молодежи), как часть процесса формирования культуры информационной безопасности, является одним из необходимых условий противодействия новым угрозам информационной безопасности.

Существенный рост числа киберпреступлений и мошенничества в сети «Интернет» в последние годы способствовал созданию на государственном уровне специализированных центров, направленных на информирование населения об актуальных угрозах информационной безопасности. Деятельность этих центров напрямую связана с формированием культуры информационной безопасности, поскольку направлена на сбор, информации об инцидентах информационной безопасности, ее анализ и дальнейшее доведение до широкого круга общественности в целях повышения осведомленности граждан о проблемах информационной безопасности. Данные центры также ведут прием информации о произошедших инцидентах, ведут консультационную и просветительскую деятельность. Помимо этого, в настоящее время существуют «горячие линии», на которые граждане имеют возможность обратиться и сообщить, как о случившемся, так и о потенциальном инциденте информационной безопасности. Необходимая информация в дальнейшем передается в правоохранительные органы, в целях расследования и привлечения к ответственности киберпреступников.

С учетом вышесказанного цель политики в области формирования культуры информационной безопасности заключается в укреплении государственных гарантий реализации конституционных прав и свобод в информационной сфере и привлечении потенциала участников информационно-телекоммуникационных взаимодействий для повышения уровня защищенности этих взаимодействий от угроз информационной безопасности. Для достижения этой цели необходимо решение следующих задач:

1. Развитие навыков безопасного поведения и взаимодействия в информационном пространстве у населения.
2. Укрепление этических норм в области информационно-телекоммуникационных взаимодействий, разработка профессиональных стандартов доверенного использования ИКТ, поддержка общественных инициатив, направленных на формирование культуры информационной безопасности, противодействие киберпреступности.
3. Создание системы информационно-консультативной помощи для противодействия инцидентам информационной безопасности и ликвидации последствие кибератак.

Таким образом, в условиях обостряющегося информационного противоборства, формирование культуры информационной безопасности требует комплексного подхода и консолидации усилий различных структур – системы образования, органов государственного управления, правоохранительных органов, бизнес-сообщества (сферы информационных технологий и информационной безопасности), а также всего общества в целом.

Заключение

Российская Федерация все активнее переходит в «экономику данных»: растет количество цифровых услуг и сервисов, повышается скорость и удобство их использования, расширяется география их предоставления. Начинают применяться технологии искусственного интеллекта, что позволяет оптимизировать некоторые производственные процессы. Вместе с этим растет и количество собираемых, хранимых и обрабатываемых данных, что в свою очередь требует все больших мощностей. С другой стороны, появляются и новые угрозы безопасности этих данных, что создает рост потребности в квалифицированных специалистах по защите информации. Проанализированные источники показывают, что повышенная потребность в таких специалистах сохраняется уже несколько лет и с каждым годом становится только больше. Кроме того, с ростом количества информационных и киберугроз простым гражданам растет и потребность в формировании у них базовых компетенций в сфере информационной безопасности. К сожалению, большинство высших учебных заведений сегодня не способны адекватно ответить на эти вызовы ввиду различных причин, связанных или с квалификацией профессорско-преподавательского состава, или с состоянием материально-технического и финансового обеспечения. В данной статье был предложен ряд мер и направлений, которые способны переломить складывающуюся ситуацию, что позволит повысить эффективность системы кадрового обеспечения сферы информационной безопасности, повысить уровень защищенности граждан и организаций от информационных и киберугроз, что в целом окажет положительное влияние на систему национальной безопасности Российской Федерации и внесет вклад в стабилизацию экономического развития страны и её субъектов.

Литература

1. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ. Статья 66.1 // URL: https://www.consultant.ru/document/cons_doc_LAW_34683/b0bc8a27e8a04c890f2f9c995f4c966a8894470e/ (дата обращения 30.07.2024).
2. Рынок коммерческих ЦОД в России 2023 // URL: https://survey.iksconsulting.ru/page30265406.html (дата обращения 30.07.2024).
3. Аналитической отчет компании F.A.C.C.T. «Киберпреступность в России и СНГ. Тренды, аналитика, прогнозы 2023-2024» // URL: https://www.facct.ru/resources/research-hub/cybercrime-trends-annual-report-2023-2024/ (дата обращения 30.07.2024).
4. Рынок труда в информационной безопасности в России в 2024-2027 гг.: прогнозы, проблемы и перспективы // URL: https://www.ptsecurity.com/ru-ru/research/analytics/preview/rynok-truda-v-informaczionnoj-bezopasnosti-v-rossii-v-2024-2027-gg-prognozy-problemy-i-perspektivy/ (дата обращения 30.07.2024).
5. Материалы исследования ЦСР «Северо-Запад» и Positive Technologies: рынок труда в ИБ ожидает структурная трансформация // URL: https://csr-nw.ru/news/detail.php?ID=2170 (дата обращения 30.07.2024).
6. Царегородцев, А. В. Кадры решают всё: назад в будущее / А.В. Царегородцев // Безопасные информационные технологии: Сборник трудов Двенадцатой международной научно-технической конференции, Москва, 01-02 ноября 2023 года. – Москва: Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет), 2023. – С. 146-149.
7. Данные корпоративной почты утекают у каждого 19-го сотрудника российских компаний // URL: https://bi.zone/news/dannye-korporativnoy-pochty-utekayut-u-kazhdogo-19-go-sotrudnika-rossiyskikh-kompaniy/ (дата обращения 30.07.2024).
8. Две трети россиян за последний год сталкивались с телефонным мошенничеством // URL: https://www.vedomosti.ru/society/articles/2024/02/20/1021201-dve-treti-rossiyan-stalkivalis-s-telefonnim-moshennichestvom (дата обращения 30.07.2024).
9. Резолюция Генеральной Ассамблеи ООН A/RES/57/239 «Создание глобальной культуры кибербезопасности» // URL: http://daccessdds.un/org/doc/UNDOC/GEN/N02/738/25/PDF/N0273825.pdf?OpenElement.
10. Малюк А.А., Полянская О.Ю., Алексеева И.Ю. Этика в сфере информационных технологий. – М.: Горячая линия – Телеком, 2011.
11. Павлова Е.Д. Медиаобразование как способ формирования национальной информационной культуры//Приоритетные национальные проекты: первые итоги и перспективы реализации//Отв. ред. Ю.С.Пивоваров. М.: ИНИОНИ РАН, 2007.

MODERN CHALLENGES TO THE PERSONNEL TRAINING SYSTEM IN THE FIELD OF INFORMATION SECURITY

Tsaregorodtsev, Anatoly Valeryevich

Doctor of science (engineering), professor
RUDN University, Center for development and maintenance of IT-solutions, director
Moscow, Russian Federation
tsaregorodtsev_av@pfur.ru

Malyuk, Anatoly Aleksandrovich

Candidate of science (engineering), professor
Moscow Engineering Physics Institute, professor
Moscow, Russian Federation
aamalyuk@yandex.ru

Volkov, Sergei Dmitrievich

RUDN University, Center for development and maintenance of IT-solutions, vice-director
Moscow, Russian Federation
volkov_sd@pfur.ru

Abstract

The article examines the impact of digitalization and digital transformation on society and connects it with the information security provision processes. For this purpose, modern challenges for the system of information security personnel training are identified. The article also analyzes the need for qualified specialists in both the field of information security and the economy of the Russian Federation as a whole. Several approaches are proposed to improve the quality of information security specialists training, and to implement this process to the existing educational system.

Keywords

digitalization; data economy; information security; personnel training; universal competencies; higher education; postgraduate education

References

1. Trudovoj kodeks Rossijskoj Federacii ot 30.12.2001 № 197-FZ. Stat'ya 66.1 // URL: https://www.consultant.ru/document/cons_doc_LAW_34683/b0bc8a27e8a04c890f2f9c995f4c966a8894470e/ (accessed on 30.07.2024).
2. Rynok kommercheskih COD v Rossii 2023 // URL: https://survey.iksconsulting.ru/page30265406.html (accessed on 30.07.2024).
3. Analiticheskoj otchet kompanii F.A.C.C.T. «Kiberprestupnost' v Rossii i SNG. Trendy, analitika, prognozy 2023-2024» // URL: https://www.facct.ru/resources/research-hub/cybercrime-trends-annual-report-2023-2024/ (accessed on 30.07.2024).
4. Rynok truda v informacionnoj bezopasnosti v Rossii v 2024-2027 gg.: prognozy, problemy i perspektivy // URL: https://www.ptsecurity.com/ru-ru/research/analytics/preview/rynok-truda-v-informaczionnoj-bezopasnosti-v-rossii-v-2024-2027-gg-prognozy-problemy-i-perspektivy/ (accessed on 30.07.2024).
5. Materialy issledovaniya CSR «Severo-Zapad» i Positive Technologies: rynok truda v IB ozhidaet strukturnaya transformaciya // URL: https://csr-nw.ru/news/detail.php?ID=2170 (accessed on 30.07.2024).
6. Tsaregorodtsev, A. V. Kadry reshayut vsyo: nazad v budushchee / A.V. Caregorodcev // Bezopasnye informacionnye tekhnologii : Sbornik trudov Dvenadcatoj mezhdunarodnoj nauchno-tekhnicheskoj konferencii, Moskva, 01-02 noyabrya 2023 goda. – Moskva: Moskovskij gosudarstvennyj tekhnicheskij universitet imeni N.E. Baumana (nacional'nyj issledovatel'skij universitet), 2023. – S. 146-149.
7. Dannye korporativnoj pochty utekayut u kazhdogo 19-go sotrudnika rossijskih kompanij // URL: https://bi.zone/news/dannye-korporativnoy-pochty-utekayut-u-kazhdogo-19-go-sotrudnika-rossiyskikh-kompaniy/ (accessed on 30.07.2024).

8. Dve treti rossiyan za poslednij god stalkivalis' s telefonnym moshennichestvom // URL: https://www.vedomosti.ru/society/articles/2024/02/20/1021201-dve-treti-rossiyan-stalkivalis-s-telefonnim-moshennichestvom (data obrashcheniya 30.07.2024).
9. Rezolyuciya General`noj Assamblei OON A/RES/57/239 «Sozdanie global`noj kul`tury` kiberbezopasnosti» // URL: http://daccessdds.un/org/doc/UNDOC/GEN/N02/738/25/PDF/N0273825.pdf?OpenElement
10. Malyuk A.A., Polyanskaya O.Yu., Alekseeva I.Yu. E`tika v sfere informacionny`x texnologij. M.: Goryachaya liniya – Telekom, 2011.
11. Pavlova E.D. Mediaobrazovanie kak sposob formirovaniya nacional`noj informacionnoj kul`tury`//Prioritetny`e nacional`ny`e proekty`: pervy`e itogi i perspektivy` realizacii//Otv. red. Yu.S.Pivovarov. M.: INIONI RAN, 2007.