

Обучение основам информационной безопасности: анализ зарубежных передовых практик

УДК 37.01:004.056



Владимир АРЧАКОВ,
заместитель
Государственного
секретаря Совета
Безопасности Республики
Беларусь, кандидат
юридических наук



Алексей БАНЬКОВСКИЙ,
начальник управления
Государственного
секретариата Совета
Безопасности Республики
Беларусь, кандидат
юридических наук



Павел САВКОВ,
главный советник
Государственного
секретариата Совета
Безопасности Республики
Беларусь

Владимир АРЧАКОВ, Алексей БАНЬКОВСКИЙ, Павел САВКОВ. Обучение основам информационной безопасности: анализ зарубежных передовых практик. В статье рассмотрены основные подходы зарубежных стран к формированию у населения базовых компетенций в сфере обеспечения информационной безопасности как составной части цифровых компетенций граждан. Отмечается ключевая роль в данном процессе профильных центров компетенций, осуществляющих проведение национальных информационно-пропагандистских кампаний, научно-методическую поддержку учреждений образования, подготовку и переподготовку преподавательских кадров и онлайн-обучение по вопросам информационной безопасности. Доказывается, что за рубежом данная образовательная деятельность является приоритетной, носит постоянный, системный характер и охватывает все социальные и возрастные группы населения.

Ключевые слова: цифровая грамотность, базовые навыки информационной безопасности, информационная безопасность, центры компетенций, онлайн-обучение.

Vladimir ARCHAKOV, Aleksei BANKOVSKY, Pavel SAVKOV. Teaching the basics of information security: Analysis of foreign best practices. The authors review the main approaches used abroad to teaching people basic information security skills as part of citizens' digital competencies and highlight the key role of competence centers in this process. These centers conduct national awareness raising campaigns, provide scientific and methodological support to educational institutions, offer training and refresher courses for teaching staff, and provide online information security training. The authors argue that such programs are attached great importance in many countries, are systemic and cover all social and age groups.

Keywords: digital literacy, basic information security skills, information security, competence centers, online training.

Повышение грамотности населения в сфере обеспечения информационной безопасности (ИБ) обусловлено необходимостью формирования устойчивости общества к новым рискам, вызовам и угрозам. Важность образования в этой сфере, особенно в условиях цифровой трансформации общества, признается как государствами, так и специализированными международными и неправительственными организациями, а также экспертным сообществом.

В Беларуси на концептуально-стратегическом уровне повышение общей компьютерной грамотности населения, включая обучение людей старшего и среднего возраста правилам пользования персональными данными, умению безопасной работы в Сети интернет, определено в качестве одного из важнейших направлений деятельности по обеспечению ИБ, наряду с подготовкой профессиональных кадров в данной сфере.

В частности, это следует из ст. 100 Концепции информационной безопасности Республики Беларусь [1]. В связи с этим изучение передового зарубежного опыта по обучению вопросам ИБ представляет особую актуальность для национальной системы образования.

Основные тенденции по формированию ключевых компетенций в сфере информационной безопасности

Трансформация образования в условиях технологической революции приводит к возрастанию потребности в т. н. «мягких навыках» или «навыках XXI века». Среди них наибольший интерес для целей настоящей работы представляют ключевые компетенции, направленные на обеспечение ИБ. Несмотря на разнообразие таких характеристик, объединяет их на-

целенность на цифровую грамотность и навыки критического мышления [2].

Цифровая грамотность определяется набором знаний и умений, которые необходимы для безопасного и эффективного использования цифровых технологий и ресурсов интернета [3]. В настоящее время на международном, региональном и национальном уровнях разработаны различные модели цифровых навыков и компетенций, которые во многом взаимно дополняют друг друга и направлены в том числе и на формирование навыков в сфере ИБ.

Модель цифровых навыков для жизни и работы [4], предложенная в 2017 году ЮНЕСКО и Международным союзом электросвязи, включает три группы, которые условно можно поделить на пользовательские и профессиональные, что также предполагает постепенный рост уровня навыков и в сфере ИБ. Пользовательские навыки, в свою очередь, включают базовые и производные. Базовые цифровые навыки связаны с функциональной грамотностью в использовании электронных устройств и приложений, включая аспекты ИБ. Специализированные профессиональные цифровые навыки связаны с регулярным решением сложных профессиональных задач в цифровой среде и составляют основу высокотехнологичных профессий в сфере ИБ, таких как специалисты по кибербезопасности, цифровому маркетингу (в т. ч. в сфере политической рекламы) и PR-коммуникациям, анализу больших данных (в т. ч. персональных).

Модель компетенций, необходимых для сотрудников в XXI веке [2], представленная в 2016 году на Всемирном экономическом форуме, включает 16 навыков, разделенных на три категории: фундаментальная грамотность, компетентности (в т. ч. критическое мышление) и свойства характера. Среди составляющих фундаментальной грамотности, содержащих навыки ИБ, – технологическая, финансовая, культурная и гражданская грамотность.

Американская модель компетенций «Структура P21. Партнерство для обуче-

ния XXI века» [2] содержит описание навыков, знаний и опыта, которые должны приобрести студенты в течение всей учебы и жизни. Одна из ключевых групп компетенций – информационные, медийные и технологические навыки (информационная, медийная, ИКТ-грамотность), что предполагает и компетенции в области ИБ.

Основная роль в разработке и продвижении концепций информационной и медийной грамотности принадлежит ЮНЕСКО и Международной федерации библиотечных ассоциаций и учреждений (ИФЛА). Быть информационно грамотным означает: человек способен понять востребованность информации и может ее найти, оценить и эффективно использовать. Стандарты по информационной грамотности для успешного обучения в этой области состоят из трех компонентов: получение, оценивание и использование информации. В контексте ИБ информационная грамотность предполагает «оценку точности и надежности информации, включая соблюдение этических норм и правил пользования полученной информацией» [5].

Также под медиаграмотностью [6] понимается совокупность навыков и умений, которые позволяют людям анализировать, оценивать и создавать сообщения в разных видах медиа, жанрах и формах. Ее ключевым аспектом является «аналитический подход к медиасреде – способность воспринимать их критически – и решимость выражать себя через медиа». По мнению экспертов, медиаграмотность включает навыки критического анализа (умение интерпретировать и понимать значение различных медиаконтентов) и навыки безопасности (умение находить выход из затруднительных ситуаций и избегать их, в том числе защита частного пространства и умение избегать вредоносных контактов и контента).

В целом информационная грамотность подчеркивает важность доступа к информации, ее оценки и этичного использования, а медиаграмотность делает акцент на способности понимать

функции медиа, оценивать качество выполнения этих функций и вступать в рациональное взаимодействие с медиа в интересах самовыражения. С 2007 года ЮНЕСКО предлагает использовать интегрированное понятие «медийная и информационная грамотность» (МИГ), поскольку в современном мире невозможно быть информационно грамотным без медиаграмотности. В 2016 году ЮНЕСКО опубликовал пять принципов МИГ, которые разъясняют характер коммуникации в медиасреде, в том числе аспекты ИБ. В подтверждение можно привести два из них:

– любая информация, независимо от ее формы представления, требует критического осмысления. Ни один формат не является более или менее значимым по сравнению с другими;

– не все знания являются правдивыми или нейтральными. У потребителей информации должна быть возможность это понять.

В данном контексте целесообразно выделить такую относительно новую и часто употребляемую дефиницию, как «информационная гигиена», под которой принято понимать свод правил безопасного поведения в цифровой среде.

В Европейском союзе цифровая компетенция с 2006 года считается одной из восьми ключевых для обучения в течение всей жизни для граждан ЕС [7]. В январе 2018 года был опубликован ряд рекомендаций по улучшению цифровой компетенции, которые расширили ее определение, включив в него написание программного кода и кибербезопасность. Этими рекомендациями также вводится понятие цифрового гражданства, обращается внимание на уязвимость персональных данных и угрозы кибербезопасности. Они также охватывают вопросы медиаграмотности (понимание языка и смыслов различных видов сообщений СМИ) и связанных с ней рисков – ложных новостей, кибербуллинга и радикализации, для противодействия которым необходимы меры по повышению осведомленности и смягчению последствий.

Деятельность ЕС в области развития цифровых навыков опирается на Рамку цифровых компетенций для граждан (DigComp), в которой предлагается подробная классификация цифровой компетентности, включающая пять областей и 21 цифровую компетенцию [8]. Данная классификация дает рекомендации для обучения людей и разработки политики в области развития цифровой экономики. При этом ряд цифровых компетенций содержат важнейшие аспекты ИБ, например такие:

– оценка данных, информации и цифрового контента предполагает способность анализировать, сравнивать и критически оценивать достоверность и надежность данных, информации, цифрового контента и их источников;

– авторские права и лицензии предполагают способность понимать, как используются авторские права и лицензии на данные, информацию и цифровой контент;

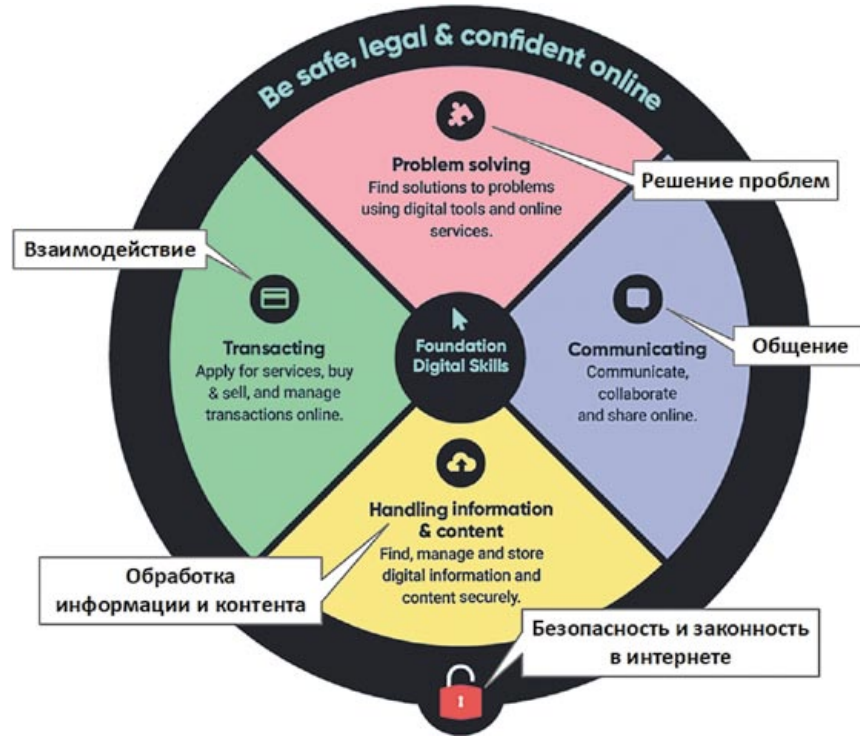
– защита устройства предполагает способность обеспечивать защиту устройств и цифрового контента, понимать риски и угрозы в цифровой среде, знать о мерах обеспечения безопасности данных;

– защита персональных данных и обеспечение конфиденциальности предполагает способность обеспечивать защиту персональных данных и конфиденциальность в цифровой среде, понимать, как пользоваться персональной информацией для предотвращения ущерба;

– защита здоровья и благополучия предполагает способность избегать рисков и угроз физическому и психологическому здоровью в процессе использования цифровых технологий, защитить себя и других от возможных опасностей в цифровой среде.

В октябре 2017 года Европейский совет призвал страны – члены ЕС привести свои системы образования и обучения «в соответствие с потребностями цифровой эпохи» [8]. Так, в Великобритании в 2018 году опубликованы Основные рамки цифровых навыков для работы и жизни онлайн, включающие пять сфер компетенций аналогично общеевропей-

► Рисунок 1. Области цифровых навыков для граждан ЕС согласно DigComp
 Источник: <https://www.etf.europa.eu>.



скому стандарту DigComp (рис. 1). Среди них отдельно выделены компетенции в сфере безопасности и законности в интернете, охватывающие все остальные категории.

Согласно документу, навыки обеспечения безопасности и законности в интернете включают следующие умения: подтвердить свою подлинность по Сети, использовать уникальные и безопасные пароли, настраивать параметры конфиденциальности сетевых учетных записей, визуально определять наличие защищенного веб-соединения, распознавать подозрительные интернет-ссылки и понимать их риски, использовать возможности резервного копирования информации в облачное хранилище или на внешний носитель. Кроме того, требуется понимать необходимость антивирусной защиты, контроля за активностью своих сетевых учетных записей, своевременного обновления программного обеспечения, соблюдения авторских и интеллектуальных прав в интернете. Документ также включает раздел о «фундаментальных» или базовых навыках, которые обычно

требуются тем, кто в настоящее время не использует цифровую технологию или использует ее ограниченными способами.

В международном исследовании «Россия 2025. От кадров к талантам» 2017 года предложена «Целевая модель компетенций 2025» [9]. В ней цифровые навыки, охватывающие технические знания в области ИКТ, рассматриваются в тесной связи с мягкими навыками и общими знаниями. При этом кибербезопасность также определена как отдельная составляющая цифровых навыков, наряду с базовой цифровой грамотностью, аналитикой данных, машинным обучением, искусственным интеллектом, программированием, архитектурой IT-систем. Отдельно в модели выделены критическое мышление и навыки работы с большими потоками информации, включая информационную гигиену и медиаграмотность, что подтверждает признание российскими экспертами важности персональных навыков противодействия дезинформации и пропаганде в медиапространстве.

Подходы зарубежных стран к формированию цифровой грамотности населения

Подходы зарубежных стран к формированию цифровых компетенций своих граждан, включая аспекты ИБ, в целом совпадают. Общепринято, что основные усилия по решению этой задачи предпринимаются прежде всего государством. Вместе с тем активное участие в реализации данного направления образовательной деятельности принимают некоммерческие организации и бизнес-организации как в инициативном порядке, так и в рамках государственно-частного партнерства (ГЧП).

На основе анализа подходов стран – членов Организации экономического сотрудничества и развития в области цифрового образования можно сделать вывод, что их деятельность по формированию цифровых компетенций осуществляется по трем направлениям: подготовка преподавателей, повышение грамотности населения и профессиональная подготовка специалистов в сфере цифровых технологий, включая аспекты ИБ. В рамках цифрового образования особое внимание уделяется созданию профильных центров компетенций, организации на их базе массовых открытых онлайн-курсов (МООК).

В Соединенных Штатах образовательная деятельность в сфере обеспечения кибербезопасности направлена на формирование у будущего поколения иммунитета к угрозам в киберпространстве, повышение цифровой грамотности взрослых и подготовку кадров в данной сфере. Так, Национальным альянсом по кибербезопасности (NCSA) совместно с Антифишинговой рабочей группой (APWG) с 2010 года проводится информационно-пропагандистская онлайн-кампания по кибербезопасности для населения «Остановись, подумай, подключайся» (Stop-Think-Connect), в которой участвуют организации не менее чем из 50 стран (в т. ч. Польши, Украины, Литвы, Латвии, Армении). В ее рамках ежегодно организуется национальный

месяц информирования о кибербезопасности. В соответствии с принятой в 2018 году Стратегией национальной кибербезопасности правительством США проводится целенаправленная работа по повышению цифровой грамотности госслужащих – организовано их обучение в сфере кибербезопасности (до 10 тыс. человек ежегодно).

В США также реализуется известная образовательная инициатива Национального научного фонда – проект «Электронный дозор» (Cyber Watch), запущенный в 2005 году в качестве регионального центра передового технологического образования в сфере кибербезопасности, а в 2012 году преобразованный в полноценный национальный центр компетенций. Среди его задач – проведение ежегодной конференции по образованию в сфере кибербезопасности; разработка и проверка образовательных стандартов и учебных программ, предусматривающих сертификацию и получение научных степеней в сфере кибербезопасности на всех уровнях университетских структур, а также проверка навыков в области кибербезопасности. Одно из новых направлений центра – обучение и поддержка перехода студентов из двухлетних в четырехлетние учебные заведения в области кибербезопасности с целью увеличения числа студентов, участвующих в другой образовательной программе «Киберкорпорация: стипендия за службу» (CyberCorps: Scholarship for Service). Цель этой программы – предоставление стипендий будущим специалистам по кибербезопасности с условием их последующего распределения на работу по специальности [10].

Агентство национальной безопасности США в интересах подготовки кадров в сфере кибербезопасности спонсирует два типа центров компетенций (Centers of Academic Excellence – CAE): киберзащиты и киберопераций, а также поддерживает центр академического мастерства разведывательного сообщества. Программа национальных центров компетенции в области киберзащиты (CAE-CD) координируется совместно с Министерством

внутренней безопасности США. Цель программы – поддержка высшего образования и научных исследований в области киберзащиты и подготовка специалистов с опытом работы в этой сфере. На 2020 год более 300 учебных заведений США получили статус центра компетенций по какому-либо направлению в области киберзащиты [11].

Программа центров компетенций в области киберзащиты и киберопераций является развитием Национальной образовательной инициативы США в области кибербезопасности NICE (The National Initiative for Cybersecurity Education), реализованной в соответствии с указом президента США Б. Обамы в 2013 году. Данная образовательная инициатива относится к ГЧП-проектам и координируется Американским национальным институтом стандартов и технологий Министерства торговли США (NIST). Ее цель – методическая поддержка интересов правительственных и бизнес-структур по созданию и развитию широкой сети образовательных учреждений и всей системы образования, обучения и подготовки кадров в области кибербезопасности. В рамках NICE разработана рамочная структура трудовых ресурсов в области кибербезопасности CWF (Cybersecurity Workforce Framework). В ее основе – единый тематический словарь терминов, который позволяет системно классифицировать и описывать компетенции работников в зависимости от вида их деятельности, специальности и должностных обязанностей применительно к сфере кибербезопасности. Важным системным компонентом рассматриваемой структуры стало включение должностей не только работников технического профиля, но и гуманитарного (юристов, экономистов и т. д.), то есть тех, кто применяет свои знания при обеспечении успешной и плодотворной работы по основным направлениям деятельности своей организации [11].

В рамках повышения цифровой грамотности взрослых в США и Великобритании под эгидой правительства созданы ряд интерактивных инструментов для

родителей (например, Joan Ganz Cooney Center), облегчающих взаимодействие с детьми в вопросах цифрового образования, в т. ч. в сфере ИБ; активно внедряются понятия «цифровой этики» и «цифровых наставников», которые, по аналогии с семейными финансовыми консультантами, помогают взрослым и детям знакомиться с современными онлайн-инструментами, оценить их возможности, риски и построить оптимальный план использования.

В Европейском союзе в январе 2018 года принят новый план действий в области цифрового образования, который включает 11 мероприятий по поддержке использования цифровых технологий и развитию цифровых компетенций в области образования [8]. Одним из таких мероприятий определена «кибербезопасность в образовании», направленная на повышение квалификации преподавателей и осведомленности обучаемых в сфере кибербезопасности. В этих целях реализуются две инициативы [12]:

- общеевропейская информационно-просветительная кампания по вопросам киберкультуры «Безопасный интернет для ЕС» (SaferInternet4EU), которая будет способствовать повышению безопасности, медиаграмотности и «кибергигиены» для детей, родителей и учителей;
- смешанный курс для учителей по кибербезопасности и педагогическим подходам к обучению кибербезопасности в начальной и средней школе (онлайн и очное обучение).

Также в рамках проекта SaferInternet4EU на базе интернет-портала «betterinternetforkids.eu» организованы:

- европейский конкурс для поощрения высококачественных ресурсов и вдохновляющих инициатив, преследующих лучшие цели интернета для детей. Конкурс охватывает три категории: профессионалы, преподаватели и молодежь;
- массовый открытый онлайн-курс по безопасности детей в интернете с ресурсами и мероприятиями для онлайн-обучения (на 6 недель), в частности по борьбе с дезинформацией, кибербуллингом и радикализацией.

Кроме того, в ЕС одной из первых и наиболее успешных глобальных инициатив в сфере формирования цифровых навыков являются Европейские компьютерные права (ECDL). Со временем этот сертификат стали называть Международными компьютерными правами (ICDL). Важно отметить, что применительно к сфере ИБ программа ECDL ограничена исключительно вопросами кибербезопасности.

Заслуживают внимания образовательные инициативы некоторых государств, направленные на подготовку специалистов по кибербезопасности со школьной скамьи. В частности, по такому пути идут в Израиле и Великобритании [13]. С четвертого класса в израильских школах дети активно изучают программирование, а одаренные старшеклассники – методы криптографии и кибербезопасности в сертифицированных центрах. Таким образом, Национальный центр киберобразования Израиля готовит профессиональный кадровый резерв для силовых ведомств, высокотехнологичной промышленности и науки. В Великобритании в рамках 5-летней национальной школьной программы осуществляется отбор нескольких тысяч учеников в возрасте от 14 до 18 лет для обучения и последующей работы в сфере ИБ. Национальный центр кибербезопасности Великобритании предлагает школьникам, родителям и учителям базовые и расширенные бесплатные курсы по ИБ в период летних каникул, а также организует ежегодные молодежные соревнования по кибербезопасности.

Наряду с вопросами безопасного использования Сети интернет в программах развития цифровой грамотности на первый план выходят компетенции критического мышления, особенно в отношении оценки достоверности информации и ее источников. Например, французская газета Le Monde разработала для своих читателей ряд интерактивных инструментов, помогающих распознавать «фейк», а также методические материалы по медиаграмотности для учителей и школьников. Журналисты

издания регулярно устраивают выездные встречи со школьниками и учат их принципам определения достоверности медиаматериалов. С 2018 года курс начал внедряться в ряде школ как обязательный. Вместе с тем экспертами отмечается [6], что процесс обучения МИГ сегодня обычно имеет спонтанный, неформальный и несистематический характер. Как правило, МИГ формируется без формального образовательного посредника. Это означает, что обучение осуществляется без специального учебного плана, практическим, индуктивным способом, без посторонней помощи, на собственных ошибках, на основе советов ровесников или подражания их поведению. Крайне редко эту информацию получают из учебников или пособий.

В целях продвижения медийной грамотности ОЭСР намерена внести изменения в свою Программу оценки знаний учащихся (Programme for International Student Assessment, PISA), на основе которой составляется международный рейтинг образовательных систем. В будущем в тесте PISA появится часть, которая позволит оценить навыки школьников по ориентированию в цифровой среде и пониманию онлайн-документов [13].

Отдельно следует выделить вклад крупных IT-компаний в повышение цифровой грамотности и кибергигиены населения (Google, Microsoft). Так, компания Google реализует ряд программ и мероприятий в области бесплатного онлайн-обучения цифровым навыкам. Это могут быть как образовательные программы совместно с правительствами стран, доступные всем гражданам, так и MOOC собственной разработки. В 2017 году Google выпустила бесплатный онлайн-курс цифрового гражданства и безопасности (Digital Citizenship and Safety Course), помогающий преподавателям обучать учеников основам безопасного поведения в Сети интернет. По завершении курса педагог получает цифровую версию учебного плана, согласно которому и будут проходить уроки цифровой грамотности в школах. Учителя, успешно окончившие курс, также

Наименование индикатора цифровой грамотности	Характеристика индикатора цифровой грамотности
Показатель информационной грамотности	Понимание роли и степени влияния информации, умение ее искать, осознание пользы или вреда
Показатель компьютерной грамотности	Навыки работы на компьютере, включая психомоторные навыки (работа с мышью и сенсорным экраном)
Показатель медиаграмотности	Проверка достоверности новостей и их источников, понимание, что новости могут освещаться предвзято
Показатель коммуникативной грамотности	Анализ позиции других людей, умение использовать современные средства коммуникации, понимание цифрового этикета
Показатель отношения к инновациям	Знания о цифровых технологиях, навыки работы с гаджетами и приложениями, понимание их пользы

▲ Таблица 1. Индикаторы цифровой грамотности населения (согласно исследованию НАФИ «Цифровая грамотность для экономики будущего») Источник: <http://nafi.ru>.

получают именной знак «Преподаватель курса «Цифровой гражданин».

В рамках повышения цифровой грамотности населения компания Microsoft разработала пять бесплатных онлайн-курсов. Среди них курс «Безопасность и конфиденциальность при работе с компьютерами». После успешной сдачи теста по материалам всех курсов выдается личный сертификат цифровой грамотности от Microsoft.

В Российской Федерации с ноября 2018 года в рамках национальной программы «Цифровая экономика Российской Федерации» [14] реализуется проект «Кадры для цифровой экономики», направленный на создание к 2024 году условий для граждан в освоении ключевых компетенций цифровой экономики, обеспечение массовой цифровой грамотности и персонализации образования. Один из шести показателей эффективности выполнения проекта в 2024 году – доля населения, обладающего цифровыми навыками, должна составить 40 % (в 2019 – 27 %). При этом понятие цифровой грамотности предполагает и аспекты ИБ.

В целях измерения уровня знаний и умений населения, необходимых для безопасного и эффективного использования цифровых технологий и ресурсов интернета в условиях цифровой экономики, в 2015–2018 годах проведен ряд исследований уровня цифровой грамотности населения. Во всероссийском исследовании «Индекс цифровой

грамотности 2017» [15], выполненном общественной организацией «Региональный общественный центр интернет-технологий» (РОЦИТ), для оценки цифровой грамотности выбраны три критерия – цифровое потребление, цифровые компетенции и цифровая безопасность. Здесь под цифровой безопасностью понимается сочетание инструментов, мер предосторожности и привычек, необходимых пользователям для гарантирования их безопасности в цифровом мире. Среди оценочных показателей цифровых компетенций отдельно обозначена компетентность в области критического восприятия информации и проверки на достоверность. Основным вывод этих исследований – развитие цифровой компетенции обостряет для пользователей проблему ИБ, что и показывает динамика индекса за весь период измерений.

В исследовании «Цифровая грамотность для экономики будущего» [16], проведенном Национальным агентством финансовых исследований (НАФИ), используется подход, предложенный в рамках саммита G20 в апреле 2017 года и базирующийся на оценке пяти индикаторов, приведенных в таблице 1. Основные выводы – 26 % россиян продемонстрировали высокий уровень базовых компетенций в цифровой среде. Риски пробелов в цифровой грамотности заключаются в неадекватной оценке роли информации в современном мире, что, в свою очередь, ведет к непониманию того, что информацию нужно защищать.

Одна из ключевых образовательных инициатив программы цифровой экономики, направленная на улучшение сложившейся ситуации, – создание, по примеру США и ЕС, центров компетенций по проблемам обеспечения ИБ, на базе которых будут функционировать МООК для образовательных учреждений и различных групп населения. Так, с конца 2019 года в России функционирует созданный в партнерстве с бизнесом бесплатный онлайн-сервис непрерывного образования взрослых «Цифровая грамотность.рф» для широких слоев населения, направленный на формирование базовых компетенций по цифровой экономике. Оператор проекта – «Университет 20.35». Среди опубликованных онлайн-материалов большинство отнесены к категории «безопасность», а раздел образовательных курсов включает такие категории, как «Цифровая безопасность» и «Медиаграмотность». В связи с созданием образовательной онлайн-платформы для отдельных типов профессиональной деятельности (например, для государственных служащих или сотрудников государственных компаний) введен механизм обязательного наличия базовых компетенций по цифровой экономике с использованием онлайн-сервиса.

В России важная роль в координации обучения граждан культуре ИБ в условиях цифровой трансформации экономики отведена правительству. Так, в рамках проведения в 2019 году Единого урока по безопасности в Сети Интернет на онлайн-платформе «www.единыйурок.рф» реализована программа для учреждений образования, позволяющая организовать преподавание ИБ обучающимся дистанционно в рамках таких учебных дисциплин, как «Информатика», «Основы безопасности жизнедеятельности», самостоятельной учебной дисциплины «Информационная безопасность», программы внеурочной деятельности и (или) дополнительного образования, программ воспитания и социализации обучающихся. Особенность реализации данной программы – дистанционное обучение ИБ по основным и дополнительным общеразвивающим программам.

К деятельности по повышению цифровой грамотности населения активно подключаются некоммерческие организации и IT-компании путем создания собственных центров компетенций, на базе которых организуется функционирование МООК и проведение информационно-просветительных и пропагандистских кампаний по вопросам ИБ. Например, «Учи.ру» – крупнейшая частная российская образовательная онлайн-платформа, на базе которой в настоящее время предоставляется бесплатный онлайн-курс повышения квалификации для педагогов «Цифровая грамотность: базовый курс по развитию компетенций XXI века» с выдачей удостоверения установленного образца. В рамках курса изучаются вопросы медиаграмотности и кибербезопасности.

Онлайн-акция по проверке знаний в области цифровых технологий «Всероссийский Цифровой Диктант 2020» на портале «digitaldictation.ru» – совместный образовательный проект РОЦИТ, общественного движения «Общероссийский народный фронт» и компании Microsoft. Диктант состоит из вопросов, разработанных с учетом разных возрастных категорий: для детей (7–13 лет), подростков (14–17 лет) и взрослых (18 лет и старше) и разделенных на четыре смысловых блока. При этом третий блок посвящен цифровой безопасности, в том числе защите персональных данных и устройств. Кроме того, среди проектов РОЦИТ, направленных на повышение навыков ИБ населения, – Центр безопасного интернета в России на портале «www.saferunet.ru», содержащий информационные материалы для детей, подростков и взрослых по тематике ИБ и посвященный проблемам безопасной, корректной и комфортной работы в интернете, а также Неделя безопасного Рунета – ежегодная информационно-просветительная и пропагандистская онлайн-акция.

Компания «Лаборатория Касперского» продвигает собственный образовательный проект «Академия Касперского» на интернет-портале «academy.kaspersky.ru»

и предлагает очные и онлайн-курсы разного уровня сложности. Их целевая аудитория – преподаватели в сфере ИБ учреждений высшего образования, руководители среднего и высшего звена, студенты и специалисты, связанные с IT-сферой, а также новички в данной сфере. Также доступна сертификация «Лаборатории Касперского» по кибербезопасности базового уровня в форме онлайн-тестирования для начинающих специалистов. В рамках другого корпоративного образовательного проекта «Академия Яндекса» продвигается бесплатный онлайн-курс «Безопасность в интернете» для школьников 6–9 классов, который также рекомендуется родителям и учителям средней школы.

В Казахстане, как и в России, обучение населения основам ИБ рассматривается как составная часть цифровой грамотности и координируется государством в рамках принятой в 2017 году программы «Цифровой Казахстан» [17]. Среди ее задач отдельно выделены две – повышение цифровой грамотности в среднем, техническом и профессиональном, высшем образовании и повышение цифровой грамотности населения (подготовка, переподготовка). При этом в Казахстане понятие цифровой грамотности в контексте ИБ ограничено, в основном, вопросами кибербезопасности.

В рамках национальной программы в 2018 году в каждом регионе Казахстана прошли бесплатные курсы по обучению населения базовым навыкам цифровой грамотности. Обучение проходило на базе школ, колледжей, библиотек – всего в 2729 учреждениях. В 2019 году, помимо четырех действующих учебных курсов базовых цифровых навыков, дополнительно введен отдельный курс «Навыки по информационной безопасности», включающий вопросы защиты персональных данных, цифровых устройств, безопасной работы в Сети интернет, а также защиты при проведении финансовых операций. Также профессиональные цифровые навыки в контексте ИБ расширяют базовый уровень цифровых компетенций за счет медиаграмотности, направленной на раз-

витие творческих способностей и критического мышления обучающихся [18].

В интересах подготовки специалистов для цифровой экономики, включая сферу ИБ, а также повышения цифровой грамотности населения в 2019 году в соответствии с поручением Елбасы создан новый IT-университет – Astana IT University. Среди его специальностей в контексте ИБ заслуживают внимания две – «Кибербезопасность» и «Цифровая журналистика», в рамках которой изучаются вопросы информационного манипулирования и медиаграмотности. С 2020 года обучение населения цифровым навыкам переводится в новый формат – за счет создания бесплатной образовательной онлайн-платформы по аналогии с российским порталом «Цифровая грамотность.рф». Также будет реализована карта площадок обучения в регионах – школы программирования, инновационные школы, курсы повышения квалификации, центры подготовки и сертификации специалистов [18].

Таким образом, из анализа мировой практики по определению ключевых навыков и компетенций населения для образования на протяжении всей жизни следует, что компетенции в сфере ИБ рассматриваются как неотъемлемая составная часть «новой грамотности» – компьютерной, информационной, медийной, цифровой. Несмотря на некоторые различия в понятиях «новой грамотности», в контексте ИБ их объединяют навыки противодействия деструктивным информационно-психологическим (критическое мышление, сетевой этикет, соблюдение законности в сети, цифровая гигиена) и информационно-техническим воздействиям (кибербезопасность). В современных условиях развитие образования в сфере ИБ подчинено интересам реализации цифровой экономики. По мере повышения цифровых навыков людей должны расти и их компетенции в сфере ИБ. Более того, обучение основам безопасности жизнедеятельности в информационной сфере должно предшествовать самому процессу получения навыков работы с ИКТ.

В целом в зарубежных странах осознается недостаточный уровень цифровой грамотности населения, в том числе и в сфере ИБ, а также ограниченные возможности учреждений образования по обучению основам цифровой безопасности. В связи с этим основные усилия направлены на развитие профильных центров компетенций, осуществляющих методическую поддержку учреждений образования, подготовку и переподготовку преподавательских кадров высшей квалификации и бесплатное онлайн-обучение по основам ИБ. Одновременно продвигается практика подтверждения работниками своих цифровых компетенций по аналогии с Европейскими компьютерными правами.

Проведенный анализ передовых образовательных практик позволяет сделать вывод: обучение основам ИБ рассматри-

вается в качестве одного из приоритетов государственной политики, носит системный характер и охватывает максимально возможный перечень социально-возрастных групп. В данный процесс вовлечены практически все заинтересованные субъекты (от международных и региональных организаций, национальных регуляторов, спецслужб, вузов до флагманов IT-индустрии, представителей малого бизнеса, волонтерских и иных общественных организаций). Представляется, что без такого комплексного проактивного подхода к развитию образования в эпоху цифровой трансформации решение задачи повышения эффективности обеспечения ИБ будет существенно затруднено. В связи с этим целесообразно учитывать зарубежный опыт в данной области в ходе совершенствования образовательного процесса в Республике Беларусь. ─

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. О Концепции информационной безопасности Республики Беларусь [Электронный ресурс]: Постановление Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1 // Национальный правовой Интернет-портал Республики Беларусь, 20.03.2019, 7/4227. – Режим доступа: <http://www.pravo.by>. – Дата доступа: 03.11.2020.
2. Мироненко, Е.С. Компетенции XXI века vs образование XXI века [Электронный ресурс] / Е.С. Мироненко // КиберЛенинка [Электронный ресурс]. – Режим доступа: <https://cyberleninka.ru/article/n/kompetentsii-xxi-veka-vs-obrazovanie-xxi-veka>. – Дата доступа: 30.10.2020.
3. Обучение цифровым навыкам: глобальные вызовы и передовые практики. Аналитический отчет к III Международной конференции «Больше чем обучение: как развивать цифровые навыки» [Электронный ресурс] // Корпоративный университет Сбербанка. 2018. – Режим доступа: <https://edutechclub.sberbank-school.ru/>. – Дата доступа: 30.10.2020.
4. Комиссия по широкополосной связи, 2017 г. Report of the Working Group on Education: digital skills for life and work: Доклад рабочей группы по вопросам образования «Цифровые навыки для жизни и трудовой деятельности» [Электронный ресурс]. – Режим доступа: <http://unesdoc.unesco.org/>. – Дата доступа: 30.10.2020.
5. Лай, Х. Руководство по информационной грамотности для образования на протяжении всей жизни [Электронный ресурс] / Х. Лай // МОО ВПП ЮНЕСКО «Информация для всех», 2006. – Режим доступа: <https://www.ifap.ru/>. – Дата доступа: 02.11.2020.
6. Педагогические аспекты формирования медийной и информационной грамотности [Электронный ресурс] // Институт ЮНЕСКО по информационным технологиям в образовании. – Режим доступа: <https://iite.unesco.org/>. – Дата доступа: 30.10.2020.
7. О ключевых компетенциях для непрерывного образования (2006/962/EC) [Электронный ресурс]: рекомендация европейского парламента и совета от 18 декабря 2006 года // Европейская Комиссия. – Режим доступа: <http://eur-lex.europa.eu>. – Дата доступа: 23.11.2020.
8. Цифровые навыки и компетенция, цифровое и онлайн обучение [Электронный ресурс] // Европейский фонд образования, Турин, 2019. – Режим доступа: <https://www.etf.europa.eu>. – Дата доступа: 30.10.2020.
9. Россия 2025. От кадров к талантам [Электронный ресурс] // The Boston Consulting Group, 2017. – Режим доступа: <http://d-russia.ru/>. – Дата доступа: 30.10.2020.
10. Взгляд на национальные и международные проблемы кибербезопасности [Электронный ресурс] // Digital.Report. – Режим доступа: <https://digital.report>. – Дата доступа: 30.10.2020.
11. Мельников, Д. К вопросу о цели и задачах национальной образовательной инициативы США в области кибербезопасности [Электронный ресурс] / Д. Мельников, Г. Гавдан, И. Корсаков // Безопасность информационных технологий = IT Security. – 2018. – Том 25. – № 2. – Режим доступа: <https://bit.mephi.ru/index.php/bit/article/view/1107>. – Дата доступа: 03.11.2020.
12. План действий в области цифрового образования – Мероприятие 7 Кибербезопасность в образовании [Электронный ресурс]. – Режим доступа: <https://ec.europa.eu/>. – Дата доступа: 30.10.2020.
13. Дети и технологии [Электронный ресурс] // Аналитический центр НАФИ, 2018. – Режим доступа: <https://naf.ru/>. – Дата доступа: 30.10.2020.
14. Цифровая экономика Российской Федерации [Электронный ресурс]: программа, утверждена постановлением Правительства РФ от 28 июля 2017 г. № 1632-р. – Режим доступа: <http://static.government.ru>. – Дата доступа: 30.10.2020.
15. Индекс цифровой грамотности 2017 [Электронный ресурс]: всероссийское исследование // Центр Интернет-технологий (РОЦИТ). – Режим доступа: <http://tocit.ru>. – Дата доступа: 30.10.2020.
16. Цифровая грамотность для экономики будущего [Электронный ресурс]: исследование // Аналитический центр «НАФИ». – Режим доступа: <http://naf.ru>. – Дата доступа: 30.10.2020.
17. Цифровая грамотность в Казахстане [Электронный ресурс] // Электронное правительство Республики Казахстан. – Режим доступа: <https://egov.kz>. – Дата доступа: 04.11.2020.
18. Что доступно казахстанцам в рамках развития цифровой грамотности [Электронный ресурс]. – Режим доступа: <https://www.zakon.kz>. – Дата доступа: 03.10.2020.

Статья поступила
в редакцию 01.12.2020 г.