УДК 004.056

Оценка уровня знаний и навыков населения Республики Беларусь в сфере информационной безопасности в условиях перехода к электронной экономике

В. С. Князькова, магистр экономических наук, магистр технических наук, преподаватель

УО «Белорусский государственный университет информатики и радиоэлектроники», ул. П. Бровки, д. 6, 220013, г. Минск, Республика Беларусь

Аннотация. Важным условием перехода к информационному обществу является доступ населения к информационно-коммуникационным технологиям (ИКТ), причем как с технической точки зрения (к примеру, возможность выхода в сеть Интернет из дома, развитие сетей нового поколения связи — LTE, 4G, 5G), так и с точки зрения достижения определенного уровня знаний и навыков в сфере ИКТ, т. е. необходимо понимание того, как именно можно использовать существующие технические возможности. По мере того, как киберпространство заполняет все большую часть нашей жизни, возрастает роль знаний и навыков также и в сфере информационной безопасности (ИБ). Статья освещает результаты исследования, проведенного на кафедре менеджмента в УО «Белорусский государственный университет информатики и радиоэлектроники», в задачи которого входила оценка знаний и навыков населения Республики Беларусь в области ИКТ, в частности, в сфере ИБ.

Ключевые слова: электронная (цифровая) экономика; сеть Интернет; информационная безопасность; навыки; навыки в сфере ИКТ

Для цитирования: Князькова, В. С. Оценка навыков населения Республики Беларусь в сфере информационной безопасности в условиях перехода к электронной экономике / В. С. Князькова // Цифровая трансформация. – 2018. – № 3 (4). – С. 34–45.

Assessing the Skills of the Population of the Republic of Belarus in the Field of Information Security in the Context of Transition to E-economy

V. S. Knyazkova, Master of Economic Sciences, Master of Technical Sciences, Lecturer

Belarusian State University of Informatics and Radioelectronics, 6 P. Brovka Str., 220013 Minsk, Republic of Belarus

Abstract. An important factor influencing the effective transition to an information society is the access of the population to information and communication technologies, both from a technical point of view (for example, the possibility of accessing the Internet from home, the development of new generation communication networks — LTE, 4G, 5G) as well as from the knowledge point of view. It is necessary to achieve a certain level of knowledge and skills in the field of ICT, i.e. it is necessary to understand how exactly the existing technical capabilities can be used. As cyberspace captures more and more in our lives, the role of knowledge and skills in the field of information security (IS) also increases. The article highlights the results of a study conducted at the Department of Management at the Belarusian State University of Informatics and Radioelectronics, which tasks included assessing the knowledge and skills of the population of the Republic of Belarus in the field of ICT, in particular, in the field of information security.

Key words: electronic (digital) economy, Internet, information security, skills, skills in the field of ICT

For citation: Knyazkova V. S. Assessing the skills of the population of the Republic of Belarus in the field of information

security in the context of transition to e-economy. *Cifrovaja transformacija* [Digital transformation], 2018, 3 (4), pp. 34–45 (in Russian).

Введение. В Республике Беларусь принят ряд нормативно-правовых документов, устанавливающих в качестве стратегического ориентира переход к электронной (цифровой) экономике. Так, Государственная программа развития цифровой экономики и информационного общества на 2016–2020 годы устанавливает следующую цель: совершенствование условий, содействующих трансформации сфер человеческой деятельности под воздействием информационно-коммуникационных технологий (ИКТ), включая формирование цифровой экономики, развитие информационного общества и совершенствование электронного правительства. В Программе также указывается, что в основе формирования цифровой экономики нашей страны лежит *надежное* и *безопасное* взаимодействие при осуществлении коммерческих транзакций *всех* участников хозяйственной деятельности (курсив автора). Таким образом, вопросы обеспечения информационной безопасности (ИБ) и защищенности всех участников трансакций являются наиважнейшими как сейчас, на этапе перехода к электронной экономической системе, так и на этапах ее дальнейшего становления и развития.

Многочисленные изменения, вызванные современной электронной средой и получившие широкое распространение посредством информационно-коммуникационной инфраструктуры, значительно расширили масштабы проблематики ИБ. Все это привело к необходимости эволюции представлений об эффективном управлении цифровой безопасностью и рисками конфиденциальности как на уровне организаций, так и на уровне стран и мирового сообщества. Повышение доверия к цифровым услугам со стороны пользователей и клиентов позволит расширить возможности их использования. Это возможно только при условии наличия определенного уровня грамотности как в целом в сфере ИКТ, так и в сфере ИБ, причем на всех уровнях социально-экономической системы страны — домашних хозяйств, организаций и государства.

Основная часть. При проведении анализа будем опираться на определение электронной (цифровой) экономики (ЭЭ), данное Беляцкой Т. Н., которая определяет ее как эволюционную стадию развития экономической системы (вслед за традиционной и индустриальной), основным фактором роста которой становится конвергенция ИКТ и иных отраслевых технологий, порождающая новую отрасль экономики – электронный бизнес [1]. ЭЭ базируется на сложной технико-технологической системе, состоящей из множества тесно связанных между собой элементов, которая, в свою очередь, основывается на ИКТ и обработке больших потоков данных («Big Data»), а также на мобильных соединениях и использовании сети Интернет, в том числе для подключения к ней огромного числа компьютеров и устройств со специальными радиочастотными метками («Интернет вещей») [2]. Расширяющиеся возможности подключения все большего числа устройств и обработки полученных данных добавляют системе сложность и зависимость от институциональных структур и процессов, которые не находятся в рамках единой юрисдикции [3, 4].

Для перехода к информационному обществу и ЭЭ необходимо эффективное использование квалифицированной рабочей силы, обладающей необходимыми навыками в самых разных областях знаний, напрямую или косвенно связанных с ИКТ. И здесь возникает ряд методологических вопросов. Какие именно навыки нужны для развития информационного общества и ЭЭ? Следует ли ограничить обучение лишь навыками в сфере инженерных и технических наук, либо есть смысл включить в «перечень» необходимых ИКТ-навыков знания и умения в сфере гуманитарных наук? Наконец, можно ли вообще создать такой перечень необходимых знаний и навыков, овладение которыми может гарантировать успех в новом, цифровом мире?

Начнем с того, что сегодня в экономической науке нет единого, универсального определения понятия «навыки». Нет такого ученого-экономиста, который бы не утверждал, что навыки трудовых ресурсов непосредственно связаны с инновационным потенциалом страны, а также с технологическими и организационными изменениями. Собственно, еще А. Смит указывал на то, что рост доли рынка ведет к специализации трудовых задач (по сути навыков) в процессах производства и к усложнению самих средств производства (что также связано с навыками) [5]. В дальнейшем так или иначе вопросы роли и значения навыков трудовых ресурсов изучались и в рамках марксистской экономической школы, и в неоклассической экономической теории. В самом общем виде

под навыком понимают способность выполнять определенную задачу, которая обычно приобретается в процессе обучения [6].

Формальной классификации навыков также пока нет. На данный момент ведущей организацией в исследовании навыков на международном глобальном уровне является Организация экономического сотрудничества и развития (ОЭСР). Она инициировала разработку, организацию и проведение нового международного сравнительного исследования взрослых, получившее название Исследование навыков взрослых как часть Программы по международной оценке компетенций взрослых (PIAAC) [7]. В отчетах ОЭСР навыки условно выделяются в четыре базовые категории: когнитивные, социальные, физические и способности к обучению [8–13]. Когнитивные включают в себя навыки чтения, математические навыки и навыки использования ИКТ. Социальные — навыки совместной работы и взаимодействия, планирования и управления временем, осуществления коммуникаций и ведения переговоров, а также общения с потребителями. Физические навыки предполагают использование непосредственно физической силы, а также сложных двигательных навыков. Навыки способности к обучению — инструктирование окружающих, навыки формального и неформального обучения, а также отслеживание изменений в профессиональной сфере деятельности человека.

Следующий вопрос заключается в том, как именно можно оценить имеющиеся у населения навыки. Сложность оценки состоит в том, что невозможно ограничиться использованием только инструмента самооценки имеющихся навыков, а ряд навыков не поддается структурированию. Кроме того, некоторые навыки (например, физические) меняются с течением времени и/или под воздействием внешних обстоятельств. Все это обуславливает сложность разработки методического инструментария комплексной оценки навыков. Обычно исследуют те навыки, которые лучше поддаются структурированию и оценке, а также те, которые в меньшей степени подвержены влиянию фактора времени и разного рода событий в жизни человека — это группа когнитивных навыков.

В настоящее время в условиях перехода к электронной экономике и информационному обществу именно навыки в сфере ИКТ играют ключевую роль. Мы можем производить самые современные аппаратные средства, проложить волоконно-оптические линии, позволяющие передавать данные с огромной скоростью, и др., но все это окажется бессмысленным без людей, которые смогут эффективно и рационально воспользоваться данной инфраструктурой. Кроме того, как уже упоминалось в начале статьи, при переходе к цифровой экономике стоит задача обеспечения надежного и безопасного взаимодействия всех ее субъектов. Вопросы, связанные с ИБ и защитой персональных данных, являются, пожалуй, самыми актуальными. Именно от того, насколько эффективно человечество их решит, зависит благополучие людей в новой цифровой реальности. Сегодня в мире все еще ведется разноплановая работа в данном направлении на уровне организации, государства и межгосударственных отношений. Создаются стандарты, правила и политики ИБ, которые активно внедряются по всему миру. Но для решения данной задачи требуется время. И сегодня вопрос недостаточного обеспечения ИБ являются одним из основных факторов, сдерживающих развитие цифровой экономики. Так, результаты исследования организаций, проведенного Национальным статистическим комитетом Республики Беларусь [14], показали, что к числу факторов, сдерживающих использование сети Интернет, 27,2 % респондентов отнесли «неудовлетворительную защиту информации от несанкционированного доступа или воздействия компьютерных вирусов», 22,1 % указали «риски, связанные с мошенничеством и другими злоупотреблениями при осуществлении электронных платежей».

Одним из базовых документов по управлению риском в цифровой экономике является Руководство по конфиденциальности ОЭСР. Под риском цифровой безопасности в нем понимают тот риск, который связан с использованием, развитием и управлением цифровой средой в процессе любой деятельности. Этот риск может быть результатом сочетания угроз и уязвимостей в цифровом окружении и привести к уменьшению эффективности социально-экономической деятельности. Риски цифровой безопасности по своей природе являются динамическими, что обусловлено физическими законами и спецификой цифрового окружения, а также участием в данных процессах человека [15]. Таким образом, участие человека в цифровых трансакциях сопряжено с рисками ИБ. Это происходит вследствие нескольких причин: хакерских атак на устройство пользователя, злонамеренных действий, низкого уровня знаний и навыков человека в сфере ИБ (ведь им обучают по сути только

специалистов; в школах на уроках информатики предусмотрено только два академических часа, посвященных данной теме). Таким образом, в рамках существующей системы образования только небольшой процент обучающихся получает хотя бы минимальную подготовку и знания в данной области. И даже среди тех, кто изучал дисциплины, связанные с ИБ и защитой информации, есть определенная часть людей, чья профессиональная деятельность непосредственно не связана с защитой информации. Поэтому у них нет мотивации постоянно актуализировать знания в данной области, т. к. они быстро устаревают — появляются и активно развиваются новые технологические среды, в которых также существуют риски и угрозы ИБ. К примеру, распространение технологии блокчейн и рост популярности майнинга привели к появлению новых видов угроз ИБ — скрытого майнинга, а также краже данных криптовалютных кошельков и обменных сервисов. Задачей злоумышленника при использовании вирусов такого типа является включение зараженного компьютера пользователя в часть распределенной сети, вычислительные мощности которой используются для добычи криптовалюты (Bitcoin, Monero, Zcash и т. п.) [16]. Заражению могут быть подвержены не только стационарные компьютеры, но и смартфоны. В наибольшей степени такой вид угрозы актуален для России, Украины и Беларуси из-за выбора языка сайтов, в которые были внедрены скрипты (доменная зона .ru и .by).

Таким образом, сегодня для успешного развития информационного общества и цифровой экономики, для обеспечения в них безопасности трансакций огромное значение приобретают знания и навыки людей в сфере ИБ. Мы сейчас не говорим про специалистов в данной области; речь идет о рядовых пользователях, которые уже сегодня совершают покупки в сети Интернет, пользуются мобильным и интернет-банкингом, общаются в социальных сетях, регистрируются на различных сайтах — участвуют и будут участвовать дальше в социально-экономической жизни цифрового общества. Как упоминалось выше, оценить навыки в сфере ИБ можно с помощью опроса. На кафедре менеджмента УО БГУИР под руководством зав. кафедрой Беляцкой Т. Н. было проведено исследование, в том числе по оценке навыков населения Беларуси в сфере ИБ. Дополнительная информация об исследовании, методике его проведения и некоторых результатах доступна в работе [17].

В исследовании респондентам предлагалось ответить на ряд вопросов по разным аспектам ИБ. Вопросы были взяты из открытых материалов ведущих IT-компаний в данной области — Лаборатории Касперского, Dr. Web, Microsoft. Структурно вопросы по знаниям и навыкам в сфере ИБ были разбиты на шесть блоков: «Самооценка», «Безопасность устройств пользователя», «Безопасность персональных данных», «Безопасность в сети Интернет», «Безопасность электронных платежей», «Безопасность в социальных сетях». Всего было опрошено 1500 человек; вопросы в сфере ИБ были предложены тем респондентам, которые при ответе на вопрос о частоте использования сети Интернет указали «в течение последних трех месяцев» и «от трех месяцев до года» (всего 1096 человек).

В блок № 1 «Самооценка» включены следующие вопросы:

1. Считаете ли Вы свои навыки работы с компьютером и сетью Интернет достаточными для того, чтобы защитить свои персональные данные (личную информацию)?

2. Считаете ли Вы свои навыки работы с компьютером и сетью Интернет достаточными для того, чтобы защитить свой компьютер (ноутбук, планшет, смартфон) от вирусной угрозы?

На эти вопросы были предложены следующие варианты ответа: «да», «нет», «не уверен(а)». Содержание остальных пяти блоков приведено в таблице 1.

Общие выводы по результатам исследования следующие.

Результаты по первому блоку вопросов «Самооценка» тесно коррелируют друг с другом. Так, уверенность в том, что имеющиеся навыки работы с компьютером и сетью Интернет достаточны для того, чтобы защитить свои персональные данные, выразили 40,3 % респондентов; уверенность в том, что имеющиеся навыки работы с компьютером и сетью Интернет достаточны для того, чтобы защитить свое цифровое устройство от вирусной угрозы, выразили 44,9 % респондентов. Мужчины уверены в своих знаниях больше, чем женщины. С точки зрения возраста, наиболее уверенными чувствуют себя респонденты в возрасте 18–24 лет — 53,6 % респондентов выразили уверенность в своих навыках по первому вопросу, по второму — 59,4 %. При переходе к следующим возрастным группам доля уверенных в своих навыках респондентов снижается и уже в возрастной группе 65–74 года составляет 26,1 % по первому вопросу, по второму — 17,4 %.

Таблица 1. Структурная схема блоков вопросов анкеты по анализу навыков в сфере ИБ
Table 1. Structural scheme of blocks of questions of the questionnaire on the analysis of skills in the field of information security

Блоки анкеты	Наименование вопроса	Варианты ответов
№ 2. Безопасность устройств пользователя	Если компьютер работает в нормальном режиме, означает ли это, что он не заражен?	Да. Если антивирус ничего не показывает, значит, вирусов нет. Если не изменилась скорость работы компьютера, значит, вирусов нет. Нет.
	Как гарантировать 100% защищенность компьютера от заражения вирусами в сети?	Таких гарантий нет. Включить брандмауэр. Установить новое программное обеспечение. Посещать только известные сайты.
	Установка одновременно нескольких антивирусных программ повышает защищенность. Вы согласны с этим?	Да, если это антивирусы одного производителя. Да, если это антивирусы от известных производителей. Да. Нет.
	Что такое Firewall, для чего он нужен?	Для фильтрации трафика. Для быстрого и безопасного поиска информации. Для очистки компьютера. Для форматирования.
	Что такое QR-код?	Матричный код, в котором может размещаться любой текст, в том числе и ссылка. Код имеет вид матрицы, содержащей черно-белое пиксельное изображение. Несмотря на то, что в матрице может размещаться любой текст, чаще всего ее используют для кодирования гиперссылок. Вредоносный код, который используется для написания вирусов. Специальный код взлома ящика электронной почты.
	Опасен ли QR-код для мобильного устройства?	Нет, не опасен — это всего лишь картинка, содержащая рекламную информацию. Не опасен, так как вирусов для QR-кодов не существует. Потенциально опасен, так как он может содержать вредоносную ссылку на принадлежащий злоумышленникам сайт или на установочный файл с вредоносной программой.
№ 3. Безопасность персональных данных	Гарантируют ли очень сложные пароли 100% защиту от нарушения конфиденциальности?	Нет. Да, если пароль не сохранен на компьютере. Да, если после работы полностью очищать файлы cookies и не хранить пароль на компьютере.
	Вы заводите новую учетную запись на каком-либо сайте. Как Вы будете выбирать пароль?	У меня один пароль на все случаи жизни. У меня несколько паролей, которые я использую для своих аккаунтов. У меня есть шаблон пароля, который я немного меняю для каждого аккаунта. Придумаю новый, посложнее.

Продолжение таблицы 1
Table 1 (continuation)

Блоки анкеты	Наименование вопроса	Варианты ответов
№ 3. Безопасность персональных данных	Сайт или сервис потребовал от Вас слишком сложный пароль. Как Вам теперь его запомнить?	Я запишу его на бумажке (в ежедневнике, записной книжке и т. п.). Придется напрячь память и его запомнить. Запомню в браузере, чтобы он сам вводил пароль. Запишу в телефон. Сохраню в текстовом файле на компьютере. Воспользуюсь специальной программой для хранения паролей.
	Как на Вашем компьютере хранится информация, которую Вы бы не хотели никому показывать?	Все конфиденциальные данные я храню в папке, защищенной паролем. Я прячу свой компьютер от посторонних Я защитил свое устройство паролем. Все конфиденциальные данные я храню в зашифрованном виде. Я прячу такие данные, только если собираюсь передать компьютер другому лицу. Я сразу удаляю все данные, которые я бы не хотел, чтобы кто-нибудь увидел. У меня нет никаких конфиденциальных данных.
	Делаете ли Вы резервное копирование Ваших данных для их последующего восстановления в случае потери с основного устройства?	Регулярно делают резервные копии только самых важных для меня файлов. У меня есть резервные копии некоторых файлов, но я не часто их обновляю. Нет, но планирую когда-нибудь. Нет, и не планирую, мне это не нужно.
	Однажды вы скачали себе приложение, а потом перестали им пользоваться. Что дальше?	Оставлю на устройстве, вдруг пригодится. Удалю. Если понадобится, скачаю заново.
	Что разрешено приложениям на Вашем мобильном устройстве?	Я не ограничиваю доступ приложений к данным на моем устройстве. Я как правило предоставляю доступ по запросу, а потом забываю. Я разрешаю доступ в зависимости от приложения и его функций. У меня нет возможности регулировать доступ приложений к данным.
	Операционная система предложила скачать и установить важные обновления, пока Вы работаете за компьютером. Ваши действия?	Не буду устанавливать. Не хочу, чтобы скорость падала. Соглашусь на установку. Вдруг что-то важное. Потом установлю, может быть. А мне операционная систем не предлагает ничего…
№ 4. Безопасность в сети Интернет	Если не нажимая на иконки просто просмотреть подозрительный сайт, ничего не произойдет. Вы согласны?	Да, простой просмотр не наносит никакого вреда. Нет. Заражение может произойти, даже если вы просто посмотрели информацию с экрана, при этом ничего не нажимая. Да, заражение происходит только после кликов, после чего запускается вирусная программа.

Продолжение таблицы 1
Table 1 (continuation)

Блоки анкеты	Наименование вопроса	Варианты ответов
№ 4. Безопасность в сети Интернет	Из каких источников Вы обычно скачиваете файлы (программы, фильмы, книги, игры)?	Я регулярно что-то скачиваю (фильмы, программы, книги) из самых разных источников. Качаю много, в основном с одних и тех же проверенных мной сайтов. Я не часто что-то скачиваю и всегда внимательно отношусь к источникам. Скачиваю только лицензионную продукцию из интернет-магазинов и магазинов приложений. Вообще ничего не качаю.
	Вы хотите скачать песню The Beatles “Yesterday” и нашли несколько вариантов в Интернете. Какие из них скачаете?	Yesterday-Beatles-Song.scr Beatles_All_songs.zip Beatles_Yesterday.mp3.exe Betles-Yesturday.wma
	Чтобы временно зарегистрироваться на новом сервисе (например, чтобы заказать разовую доставку), Вам необходимо указать своей e-mail. Какую почту вы укажете?	У меня одна почта. Я везде ее указываю. У меня есть специальная почта для таких случаев, укажу ее. Укажу рабочую.
	Как Вы относитесь к тому, что сайты, которые Вы посещаете, автоматически определяют не только Ваше местоположение, но и предлагают Вам рекламу, основанную на том, какие сайты Вы посещаете и какие слова ищете в поисковиках?	Мне это нравится, очень удобно! Мне это не очень нравится, но что уж с этим поделаешь — таков Интернет. Я активировал(а) функцию запрета «слежения» в браузере и пользуюсь «приватным режим» при поиске. Я установил(а) специальное приложение/плагин для предотвращения отслеживания сайтами. Я никогда не обращал(а) на это внимания.
	Сохраняется ли у Вас в браузере история посещения страниц?	Я отключил(а) такую возможность. Да, но я ее регулярно чищу. Да. Ведь это удобно. Браузер сам предлагает мне ссылки, пока я их набираю. Не знаю.
№ 5. Безопасность электронных платежей	Вы хотите приобрести книги, оплатив покупку онлайн. Какие из перечисленных ниже средств обеспечивают безопасность онлайн-транзакций на сайте?	Антивирусное программное обеспечение. Протокол SSL. Брандмауэр Windows. Файлы cookie.
	Вы решили расплатиться в кафе банковской картой. Какой вариант Вас устроит?	Официант возьмет мою банковскую карту со счетом на кассу, а потом принесет мне чек. Официант подойдет с терминалом к моему столику и при мне произведет все операции. Официант спишет номер и CVV карты и провести платеж позднее, чтобы не задерживать меня.

Продолжение таблицы 1
Table 1 (continuation)

Блоки анкеты	Наименование вопроса	Варианты ответов
№ 5. Безопасность электронных платежей	Предположим, Вы являетесь клиентом банка MoneyBank и хотите провести онлайн трансакции. Для этого Вам необходимо авторизоваться на сайте банка. В адресной строке Вы видите следующие данные. На какой странице (или страницах) авторизация будет максимально безопасной?	http://MoneyBank.com https://MoneyBank.com https://MoneyBarnk.com https://MoneyBank.abc.com Никогда не авторизуюсь на сайтах банков.
	Некто Бекмурат Жапаркулов хочет задать пароль для своей учетной записи онлайн-банкинга. Какой из перечисленных ниже паролей является надежным?	Пароль АБВ ЖБекмурат#175 БекмуратЖапаркулов
	Как злоумышленники могу украсть PIN-код банковской карты?	Коды могут быть похищены в результате утечки данных (например, данные могут быть украдены сотрудниками банка, базы с кодами могут быть украдены в результате хакерской атаки). С помощью троянской программы, внедренной в программное обеспечение банкомата (ATM). Причем хозяин троянца может централизовано получать данные об украденных кодах во всех банкоматах взломанной сети банка. С помощью специального устройства — скиммера, которым тайно оборудуется банкомат.
№ 6. Безопасность в социальных сетях	Есть ли у Вас страничка в какой-нибудь социальной сети (Facebook, Twitter, Instagram, Flickr, Tumblr, Vkontakte и тому подобные)?	Да. Нет.
	От друга в социальной сети Вам прилетела просьба пройти по ссылке и лайкнуть фотки. Как Вы поступите?	Перейду, конечно! Это же мой друг. Напишу ему/ей в ответ просьбу поподробнее рассказать, что за фотографии лежат по ссылке? Если он/она ответит, то открою. Помечу сообщение как «спам» и добавлю друга в игнор-лист.
	Что Вы делаете, если в социальной сети Вам приходит сообщение с просьбой добавить в друзья от незнакомого человека?	Обычно я добавляют в друзья всех желающих, чем больше людей в друзьях – тем лучше. Добавляю, если человек – друг моего друга. Я добавляю в друзья только тех людей, которых знаю лично.
	Какая информация о Вас в социальных сетях находится в открытом доступе, то есть видна не только друзьям?	Только ФИО и фотография, все остальное закрыто для просмотра. Много всего, я не ограничиваю настройки видимости. ФИО, фотографии, посты. ФИО, фотографии, посты, геометки и чекины. Я никогда не задумывался/задумывалась об этом.

Самый высокий результат в самооценке своих навыков в сфере ИБ зафиксирован в г. Гродно и Гродненской области; минимальный — в г. Витебске и Витебской области. На самооценку навыков респондентов в сфере ИБ практически не влияет тип населенного пункта респондента.

На наш взгляд, достаточно интересными получились результаты в разрезе образования респондентов. Наиболее высоко свои знания и навыки оценили люди, закончившие аспирантуру и/или докторантуру (и в том, и в другом случае — 66,7 % респондентов). За ними следуют респонденты с базовым образованием. Самый низкий процент здесь у респондентов с высшим образованием. Такие результаты можно объяснить тем, что люди с более высоким уровнем образования имеют больше представления о том, с какими видами угроз можно столкнуться в киберпространстве, а также о том, что полностью защитить данные и цифровые устройства невозможно; получается, как у Сократа: «Я знаю только то, что ничего не знаю, но другие не знают и этого». Это не относится к респондентам, которые окончили аспирантуру и/или докторантуру — по нашему мнению, именно они обладают максимальным потенциалом для защиты в киберпространстве.

Таким образом, чуть более 40 % респондентов считают свои навыки работы с компьютером и сетью Интернет достаточными для того, чтобы защитить свои персональные данные, а также защитить свой компьютер (ноутбук, планшет, смартфон) от вирусной угрозы. Такой результат не может считаться высоким в современных реалиях — больше половины респондентов считают, что им недостает знаний и навыков в области ИБ.

Дадим общую характеристику ответам респондентов на вопросы анкеты по блоку ИБ. Самое большое число правильных ответов было получено по блоку 2 «Безопасность устройств пользователя» (62,57 %); минимальное число правильных ответов респонденты дали на вопросы блока 4 «Безопасность в сети Интернет» (33,77 %) (рисунок 1).

На знания и навыки в сфере ИБ значимого влияния не оказывают следующие факторы: пол, тип населенного пункта (городской либо сельский). Доля респондентов, правильно ответивших на вопросы анкеты, минимальна в г. Бресте и Брестской области и максимально в г. Минске (чаще всего, но не всегда). Отметим, что в большинстве случаев результаты распределены достаточно равномерно по областям

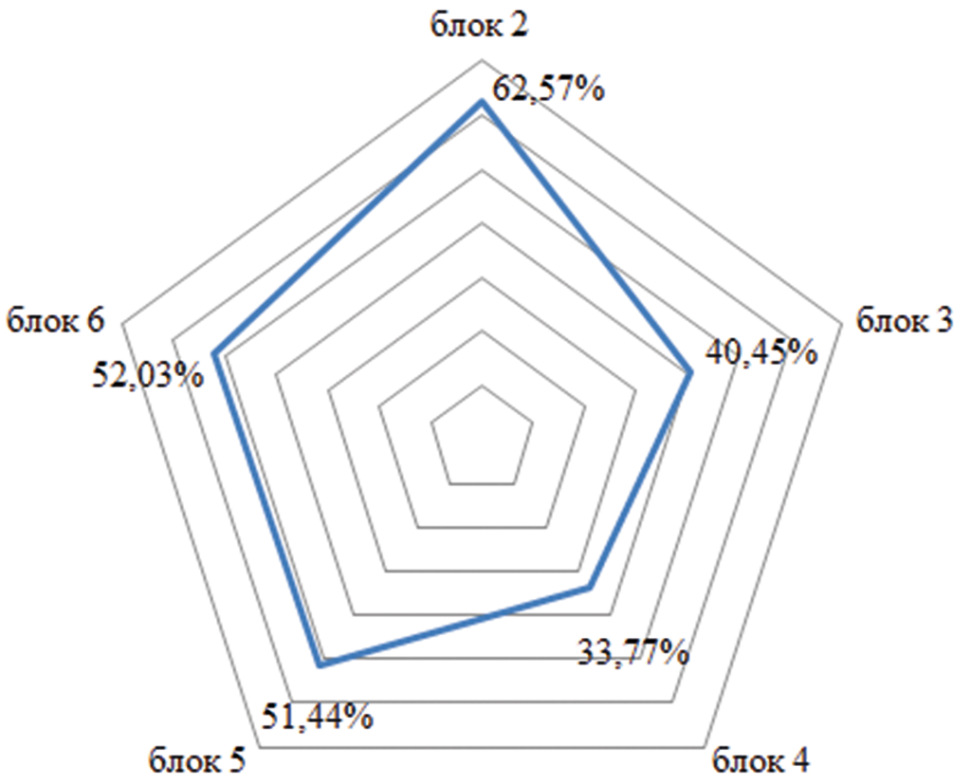

Рис. 1. Распределение доли респондентов, давших правильные ответы, по блокам анкеты
Fig. 1. The distribution of the proportion of respondents who gave correct answers on the blocks of the questionnaire

Беларуси. Обычно больше правильных ответов давали более молодые респонденты, а также респонденты с более высоким уровнем образования.

Заключение. Обеспечение защиты и конфиденциальности данных является основой дальнейшего развития всех подсистем электронной экономики. Помимо разработки политик и стандартов в данной области на уровне государств и организаций, важным элементом системы ИБ электронной экономики являются знания и навыки в данной сфере всех ее участников, как профессионалов, так и обычных пользователей.

В связи с вышесказанным вопросы повышения грамотности населения Республики Беларусь в сфере ИБ следует решать на государственном уровне. Во многих странах задача повышения грамотности людей в целом в сфере ИКТ является приоритетной. Так, по оценкам Европейской комиссии, в будущем на 9 из 10 рабочих мест людям будут необходимы т. н. «цифровые» навыки; при этом 44 % европейцев в возрасте от 16 до 74 лет не имеют этих навыков вообще. В ряде стран вопросы приобретения и актуализации знаний в сфере ИКТ выдвигаются на первый план — к примеру, в России в рамках программы «Цифровая экономика» планируется осуществить ряд проектов по обучению и повышению грамотности населения в области ИБ; общие затраты федерального бюджета на проекты в этой сфере в 2018–2019 гг. составляют 2,63 млрд. российских рублей [18].

Для повышения уровня знаний населения в сфере ИКТ в целом и ИБ в частности необходим целый комплекс мероприятий. По нашему мнению, начать следует со следующего. Во-первых, увеличить количество часов, выделяемых в школе на вопросы, связанные с проблематикой ИБ. Во-вторых, ввести в государственный компонент учебных планов предмет «Основы информационной безопасности» в средних специальных и высших учебных заведениях. В-третьих, создать некоммерческую платформу, которая бы являлась электронным посредником между ИТ-специалистами и рядовыми пользователями, предлагая последним видео-уроки, учебную литературу, мастер классы по использованию современных цифровых технологий. Реализация данных мероприятий не требует существенных капиталовложений, при этом будут заложены основы образовательной системы, способствующей повышению знаний и навыков в сфере ИКТ.

Список литературы

1. Беляцкая Т. Н. Методики сравнительного анализа систем электронной экономики // Международный научно-исследовательский журнал. – 2017. – № 10 (64). – С. 75–84.
2. Data-Driven Innovation: Big Data for Growth and Well-Being [Electronic resource]. – Paris, OECD Publishing, 2015. – Mode of access: http://dx.doi.org/10.1787/9789264229358-en. – Date of access: 01.03.2018.
3. Managing digital security and privacy risk. Background report for Ministerial Panel 3.2 [Electronic resource]. – OECD Directorate for science, technology and innovation, Committee on digital economy policy, 2016. – Mode of access: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG (2016)1/FINAL&docLanguage=En. – Date of access: 01.03.2018.
4. OECD Digital Economy Outlook 2017 [Electronic resource]. – Paris, OECD Publishing, 2017. – Mode of access: http://dx.doi.org/10.1787/9789264276284-en. – Date of access: 01.03.2018.
5. Toner, P. Workforce Skills and Innovation: An Overview of Major Themes in the Literature [Electronic resource] / P. Toner // OECD Education Working Papers. – 2011. – № 55. – Mode of access: https://www.oecd-ilibrary.org/docserver/5kgk6hpnhxzq-en.pdf?expires=1534184864&id=id&accname=guest&checksum=E93915940903049CB056230F35027DBC. – Date of access: 13.08.2018.
6. A Literature Review on Skills and Innovation. How Does Successful Innovation Impact on the Demand for Skills and How Do Skills Drive Innovation? [Electronic resource] / B. Tether [et al.]. – University of Manchester, 2005. – Mode of access: https://www.researchgate.net/publication/268212425/download. – Date of access: 13.08.2018.
7. Technical Report of the Survey of Adult Skills (PIAAC) [Electronic resource]. – OECD, 2013. – Mode of access: https://www.oecd.org/skills/piaac/_Technical%20Report_17OCT13.pdf. – Date of access: 20.04.2017.
8. OECD Skills Outlook 2015: Youth, Skills and Employability [Electronic resource]. OECD Publishing, 2015. – Mode of access: http://www.mecd.gob.es/dctm/inee/internacional/1-skillsoutlook2015.pdf?documentId=0901e72b81d77c93. – Date of access: 23.06.2017.
9. Literacy, Numeracy and Problem Solving in Technology-Rich Environments: Framework for the OECD Survey of Adult Skills [Electronic resource]. – OECD Publishing, 2012. – Mode of access: http://dx.doi.org/10.1787/9789264128859-en. – Date of access: 21.04.2017.
10. Skills for a digital world. Panel 4.2 [Electronic resource]. – Mode of access: https://www.oecd.org/internet/ministerial/

meeting/Skills-for-a-Digital-World-discussion-paper.pdf. – Date of access: 22.06.2017.
11. Skills for a Digital World [Electronic resource]. – Mode of access: https://www.oecd.org/els/emp/Skills-for-a-Digital-World.pdf. – Date of access: 22.06.2017.
12. Skills for a Digital World: 2016 Ministerial Meeting on the Digital Economy Background Report [Electronic resource] // OECD Digital Economy Papers. – 2016. – № 250. – Mode of access: http://www.oecd-ilibrary.org/docserver/download/5jlwz83z3wnw-en.pdf?expires=1498168148&id=id&accname=guest&checksum=C3530CFF26231F3675C252C1F4B07D38. – Date of access: 23.06.2017.
13. Technical Report of the Survey of Adult Skills (PIAAC) [Electronic resource]. – OECD, 2013. – Mode of access: https://www.oecd.org/skills/piaac/_Technical%20Report_17OCT13.pdf. – Date of access: 20.04.2017.
14. Информационное общество в Республике Беларусь [Электронный ресурс]. – Минск: Национальный статистический комитет Республики Беларусь, 2015. – Режим доступа: http://www.belstat.gov.by/ofitsialnaya-statistika/publications/izdania/public_compilation/index_721/. – Дата доступа: 16.12.2016.
15. Guide for conducting risk assessment. Special publication 800-30, revision 1 [Electronic resource]. – NIST, 2012. – Mode of access: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf. – Date of access: 02.03.2018.
16. Лыньков, Л. М. Майнинг криптовалют: новые вызовы информационной безопасности / Л. М. Лыньков, В. С. Князькова // Технические средства защиты информации: тезисы докладов XVI Белорусско-российской научно-технической конференции, Минск, 5 июня 2018 г. / Белорус. гос. ун-т информатики и радиоэлектроники; редкол.: Т. В. Борботько [и др.]. – Минск, 2018. – С. 59–60.
17. Князькова, В. С. Методика исследования интеллектуальной составляющей электронной экономики / В. С. Князькова // Цифровая трансформация. – 2018. – № 2 (3). – С. 19–28.
18. На обучение россиян информационной безопасности просят 2,6 миллиарда [Электронный ресурс]. – Режим доступа: http://safe.cnews.ru/news/top/2017-12-01_na_obuchenie_rossiyan_informatsionnoj_bezopasnosti. – Дата доступа: 01.09.2018.

References

1. Beliatskaya, T. N. Methods of comparative analyses of e-economy systems. Mezhdunarodnyi nauchno-issledovatelskii zhurnal [International Scientific and Research Journal], 2017, no. 10 (64), pp. 75-84 (in Russian).
2. Data-Driven Innovation: Big Data for Growth and Well-Being. OECD Publishing, Paris, 2015, 456 p. Available at: http://dx.doi.org/10.1787/9789264229358-en (accessed: 01.03.2018).
3. Managing digital security and privacy risk. Background report for Ministerial Panel 3.2. OECD Directorate for science, technology and innovation, Committee on digital economy policy, 2016, 42 p. Available at: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2016)1/FINAL&docLanguage=En (accessed: 01.03.2018).
4. OECD Digital Economy Outlook 2017. OECD Publishing, Paris, 2017, 324 p. Available at: http://dx.doi.org/10.1787/9789264276284-en (accessed: 01.03.2018).
5. Toner, P. Workforce Skills and Innovation: An Overview of Major Themes in the Literature. OECD Education Working Papers, 2011, no 55. Available at: https://www.oecd-ilibrary.org/docserver/5kgk6hpnhxzq-en.pdf?expires=1534184864&id=id&accname=guest&checksum=E93915940903049CB056230F35027DBC (accessed: 13.08.2018).
6. Tether B. A Literature Review on Skills and Innovation. How Does Successful Innovation Impact on the Demand for Skills and How Do Skills Drive Innovation. University of Manchester, 2005. Available at: https://www.researchgate.net/publication/268212425/download (accessed: 13.08.2018).
7. Technical Report of the Survey of Adult Skills (PIAAC). OECD, 2013. Available at: https://www.oecd.org/skills/piaac/_Technical%20Report_17OCT13.pdf (accessed: 20.04.2017).
8. OECD Skills Outlook 2015: Youth, Skills and Employability. OECD Publishing, 2015. Available at: http://www.mecd.gob.es/dctm/inee/internacional/1-skillsoutlook2015.pdf?documentId=0901e72b81d77c93 (accessed: 23.06.2017).
9. Literacy, Numeracy and Problem Solving in Technology-Rich Environments: Framework for the OECD Survey of Adult Skills. OECD Publishing, 2012. Available at: http://dx.doi.org/10.1787/9789264128859-en (accessed: 21.04.2017).
10. Skills for a digital world. Panel 4.2. Available at: https://www.oecd.org/internet/ministerial/meeting/Skills-for-a-Digital-World-discussion-paper.pdf (accessed: 22.06.2017).
11. Skills for a Digital World. Available at: https://www.oecd.org/els/emp/Skills-for-a-Digital-World.pdf (accessed: 22.06.2017).
12. Skills for a Digital World: 2016 Ministerial Meeting on the Digital Economy Background Report. OECD Digital Economy Papers, 2016, № 250. Available at: http://www.oecd-ilibrary.org/docserver/download/5jlwz83z3wnw-en.pdf?expires=1498168148&id=id&accname=guest&checksum=C3530CFF26231F3675C252C1F4B07D38 (accessed: 23.06.2017).
13. Technical Report of the Survey of Adult Skills (PIAAC). OECD, 2013. Available at: https://www.oecd.org/skills/piaac/_Technical%20Report_17OCT13.pdf (accessed: 20.04.2017).
14. Informacionnoe obshhestvo v Respublike Belarus' [Information society in the Republic of Belarus]. Minsk, National Statistical Committee of the Republic of Belarus, 2015. Available at: http://www.belstat.gov.by/ofitsialnaya-statistika/

publications/izdania/public_compilation/index_721/ (accessed: 16.12.2016) (in Russian).
15. Guide for conducting risk assessment. Special publication 800-30, revision 1. NIST, 2012. Available at: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf (accessed: 02.03.2018).
16. Lynkov, L. M., Knyazkova, V. S. Mining crypto: new challenges to information security. Tekhnicheskiye sredstva zashchity informatsii: tezisy dokladov XVI Belorussko-rossiyskoy nauchno-tekhnicheskoy konferentsii [Technical Means of Information Protection: Abstracts of the XVI Belarusian-Russian Scientific and Technical Conference], Minsk, 2018, pp. 59–60 (in Russian).
17. Knyazkova, V. S. Methods of intellectual perspective of e-economy. Tsyfrovaia transformatsia [Digital Transformation], 2018, 2 (3), pp. 19–28 (in Russian).
18. Na obuchenie rossijan informacionnoj bezopasnosti prosjat 2,6 milliarda [For the education of Russians in the field of information security 2.6 billion is requested]. Available at: http://safe.cnews.ru/news/top/2017-12-01_na_obuchenie_rossiyan_informatsionnoj_bezopasnosti (accessed: 01.09.2018) (in Russian).

Received: 21.08.2018 *Поступила: 21.08.2018*