ЦИФРОВАЯ ГРАМОТНОСТЬ НАСЕЛЕНИЯ

Развитие всех сфер современного общества в последние годы характеризуется значительными изменениями, вызванными цифровизацией. Положительные тенденции цифровизации несомненны: переход трудовой деятельности, образования, медицины в онлайн-среду, снижение издержек на поиск информации, повышение производительности труда за счет привлечения цифровых технологий, использование систем, заменяющих человека, в опасных для жизни и здоровья производствах, совершение онлайн-покупок, улучшение доступности государственных услуг для граждан и др. Значимость цифровых технологий определяется тем, что использование их потенциала позволяет сконструировать новый цифровой мир. Однако его успешное функционирование невозможно без людей, обладающих высоким уровнем цифровой грамотности.

В 2011 г. ООН опубликовала доклад, в котором право на доступ к сети Интернет признается неотъемлемым правом человека. В докладе в качестве основных барьеров доступа и использования сети Интернет рассматриваются свобода доступа к контенту и к инфраструктуре. Несомненно, страны мира различаются по уровню развития инфраструктуры информационно-коммуникационных технологий (далее – ИКТ), а именно: по степени покрытия стран волоконно-оптическими линиями связи, по численности серверов и пр. Они различаются и по свободе доступа к контенту, например проект «Золотой щит», представляющий собой систему фильтрации контента сети Интернет в Китае, в результате работы которого заблокирован доступ к таким популярным сайтам, как YouTube, Flickr, Facebook, Instagram, а также к некоторым новостным ресурсам и СМИ – Reuters, Wall Street Journal, Bloomberg). При этом необходимо отметить, что Республика Беларусь придерживается позиции свободного доступа к информации новостного и развлекательного характера (указанные ресурсы доступны в национальном сегменте сети Интернет).

Несмотря на актуальность названных аспектов доступа к сети Интернет, особую значимость приобретает когнитивная сторона доступа и использования ИКТ. Овладение основами и навыками цифровой грамотности сегодня актуально для каждого человека. Тому, кто не умеет пользоваться современными информационными технологиями, приходится очень непросто, так как это неумение оборачивается отсутствием выгод, например, услуг интернет-банкинга, бесплатных международных звонков и т.д., а в ряде случаев приводит к прямым потерям. Они могут быть весьма ощутимыми, как, например, потеря работы для аналитика, если у него отсутствуют компетенции, позволяющие определять достоверные источники информации. Цифровая грамотность позволяет продуктивно трудиться и реализовывать свои цели в условиях повсеместного использования цифровых технологий. Для Республики Беларусь, активно внедряющей цифровые технологии во все сферы жизнедеятельности общества и нуждающейся в кадрах, обладающих знаниями и развитыми навыками цифровой грамотности, рассматриваемые аспекты приобретают особое значение.

Термин «цифровая грамотность» впервые был введен П.Гистлером, который определял его как способность пользоваться информацией, представленной с помощью компьютера. ООН определяет цифровую грамотность как способность безопасным и должным образом получать доступ, управлять, понимать, интегрировать, общаться, оценивать и создавать информацию с помощью цифровых технологий для трудоустройства, создания достойных рабочих мест и предпринимательства. Сегодня в отечественной науке применяется подход к определению цифровой грамотности как интегрального показателя, включающего информационную, компьютерную, коммуникативную, медийную грамотность (медиаграмотность) и отношение к технологическим инновациям. Соответственно, оценка данных компонентов определяет уровень владения цифровой грамотностью. Именно от степени подготовленности к цифровым изменениям зависит включенность в процессы цифровизации, наряду с такими факторами, как психологические установки, способности рефлексии, барьеры восприятия инноваций и др.

Выделяют различные аспекты цифровой грамотности, к которым относят вопросы кибербезопасности, информационной грамотности, пользования техническими средствами, онлайн-обучения, а также этики и культуры коммуникации в сети Интернет.

Информационная грамотность – способность эффективно находить, анализировать и оценивать информацию из разных источников в интернете. Необходимость уметь фильтровать ложные и недостоверные данные, понимать источники и авторитетные ресурсы является ключевой задачей в эпоху переполнения информацией.

Безопасность в Сети (кибербезопасность) становится критически важной составляющей цифровой грамотности. Пользователи должны уметь защищать личные данные, понимать риски мошенничества, знать о способах защиты устройств от вирусов и фишинговых атак, а также о правилах создания безопасных паролей и сохранения конфиденциальности.

Умение пользоваться современными мобильными устройствами и их функциями, включая использование приложений для повседневных задач (банковские сервисы, социальные сети, образование и развлечения), является важной частью цифровой грамотности, что позволяет экономить время путем совершения транзакций, получения услуг несколькими кликами, не обращаясь в банковское учреждение или государственную организацию (например, сервис «Е-паслуга»).

Онлайн-образование обусловлено тем, что современные технологии позволяют получать знания и развивать навыки через онлайн-курсы и платформы. Овладение этими инструментами способствует личностному и профессиональному развитию, делает образование доступным для широкой аудитории, включая самые незащищенные слои населения (например, лица с ограниченными возможностями).

С развитием цифровых технологий возникает вопрос о культурных и этических нормах общения в Сети. Этика и культура общения в сети Интернет включает в себя осведомленность о правилах цифрового этикета, уважительное

отношение к другим пользователям, соблюдение авторских прав и ответственный подход к публикации контента.

Несколько лет назад высказывалось мнение, что процессы социального взаимодействия в Сети находятся даже не в стадии первичного осмысления представителями социальных наук (социологов, философов, психологов), а в стадии возникновения интереса к этой проблеме. Если в конце первого десятилетия интерес только зарождался, то сегодня широкие исследования цифровой грамотности населения проводятся повсеместно.

Регулярные исследования готовности населения к изменениям в цифровой сфере проводятся и в Беларуси. В частности, цифровая грамотность оценивалась в ходе исследования, проведенного Институтом социологии НАН Беларуси в августе-сентябре 2022 г. в рамках мониторинга методом личного опроса по месту жительства. Общий объем выборки составил 1848 человек в возрасте 18 лет и старше. Использовалась республиканская многоступенчатая стратифицированная выборка. Инструментарий исследования содержал вопросы, направленные на получение информации по ряду тематических областей, в том числе в области цифровой грамотности.

Согласно полученным данным, 73,4 % респондентов, мужчины (74,4 %) и женщины (72,6 %), пользуются Интернетом практически каждый день. Ожидаемыми результатами оказалась возрастная дифференциация: Интернет является основным каналом общения для подавляющего большинства респондентов в возрасте от 18 до 29 лет и от 29 до 49 лет (92,9 % и 90,1 % соответственно) и только для половины респондентов в возрасте 50 лет и старше – 51,0 %.

Постулат о том, что цифровая грамотность, как и общая грамотность человека, не имеет профессии, так как это система знаний, навыков и установок в области повседневного использования цифровых технологий, подтверждает данные нашего опроса. Они свидетельствуют о том, что Интернет освоили представители всех 15 сфер профессиональной деятельности, указанных респондентами: бытовое обслуживание и общественное питание, государственное управление, информационные технологии, культура и досуг, здравоохранение, милиция, армия и другие силовые структуры, наука, образование, промышленность, сельское хозяйство, СМИ, строительство, торговля, туризм и спорт, финансово-банковская сфера.

В первую пятерку вошли сферы государственного управления и СМИ, 100 % представителей которых используют Интернет практически каждый день. Ожидалось, что все представители IT-индустрии ежедневно пользуются Интернетом, однако таковых оказалось 97,0%. Пятерку замыкают представители сферы туризма и спорта (92,3 %) и силовых структур (90,0 %). Высокие показатели (от 86,8 % до 78,4 %) также демонстрируют представители других сфер профессиональной деятельности: торговли, медицины, науки, образования, бытового обслуживания, промышленности и строительства, и только сфера сельского хозяйства является исключением (55,6% представителей используют Интернет каждый день).

Как правило, белорусы предпочитают общение в мессенджерах (Viber, WhatsApp, Telegram) (66,8 %) и социальных сетях (58,9 %), а их общение по электронной почте, на форумах, в чатах и по скайпу случается гораздо реже (25,7 %, 15,2 % и 13,0 % соответственно).

Другое исследование, проведенное в БГУИР, во-первых, позволило оценить уровень цифровой грамотности населения Республики Беларусь, во-вторых, подтвердило наличие цифрового разрыва по данному фактору. В результате исследования были получены результаты по неудовлетворительному уровню цифровой грамотности в сфере информационной безопасности – общая средняя оценка составила 5,4 балла (по 10-балльной шкале).

Как отмечается в научных трудах, вопрос об обеспечении безопасности личных данных связан с формированием компьютерных навыков. Согласно полученным данным в проводимых исследованиях, навыки эффективной работы с компьютером как средством и инструментом у белорусского населения невысоки. Каждый третий респондент (37,0 %) указал, что не умеет делать ничего из перечисленного в анкете, и в этом показателе весомая доля ответов принадлежала пожилым респондентам (62,7 %). Менее половины респондентов (47,4 %) умеют изменять личные пароли на компьютере и в онлайн-сервисах, каждый третий – проверять компьютер на вирусы (35,5 %), проводить чистку компьютера от ненужных файлов (34,4 %), чистить историю браузера (34,3 %), каждый четвертый – изменять настройки доступа к своей информации в социальных сетях для разных групп пользователей (25,4 %), каждый пятый – делать резервные копии хранящихся на компьютере файлов (19,2 %). Всего 14,0 % респондентов могут создавать несколько учетных записей пользователей одного компьютера, и только 11,9 % – осуществлять функции родительского контроля на компьютере. Можно отметить проявления половозрастных отличий: указанные навыки оказались более сформированными у респондентов мужского пола и респондентов в возрасте от 18 до 29 лет. Кроме того, различия в вопросе формирования компьютерных навыков, необходимых для обеспечения безопасности личных данных, выявлены и у респондентов, проживающих в разных типах населенных пунктов: горожане владеют такими навыками в более высокой степени, чем сельские жители.

В этой связи практические рекомендации по обеспечению информационной безопасности как элемента цифровой грамотности в повседневной деятельности и в быту можно представить в виде совокупности мероприятий.

Безопасность электронной почты (E-mail) обеспечивается посредством:

подключения двухфакторной аутентификации;

использования надежного пароля для доступа к E-mail; использования спам-фильтров;

использования как минимум двух типов отдельных e-mail адресов: закрытых (только для интернет-банкинга, привязки устройств и средств защиты

и т. д.), открытых (только для переписки, регистрации на форумах и социальных сетях, оформления различных подписок и т. д.);

в случае подозрительных ситуаций проверки статистики подключений и изменения пароля.

Не рекомендуется реагировать на письма от неизвестных отправителей, открывать подозрительные вложения к письму (при необходимости вложенные ссылки либо файлы следует проверять на наличие вирусов с помощью специализированных онлайн-сервисов, а также не рекомендуется отправлять в открытом виде важные данные (фотоизображения документов, пароли и т. д.).

Безопасность средств парольной защиты создается путем:

создания персональных (уникальных) паролей к разным сервисам;

использования сложных паролей (например, одновременно будут строчные и заглавные буквы, цифры, специальные знаки (~ ! @ # $ % & *);

регулярной смены паролей.

Не рекомендуется хранить пароли на бумажных носителях, рабочем столе компьютера и в других легкодоступных местах, а также передавать их кому-либо; использовать повторения символов; использовать в качестве пароля свой логин (имя пользователя, учетной записи, никнейм, дату рождения и т. д.); сохранять пароль автоматически в браузере; использовать биографическую информацию и сведения, размещенные в социальной сети.

Безопасность в сети Интернет обеспечивается посредством:

использования только защищенных соединений HTTPS (наличие в адресной строке браузера зеленой или серой иконки замка);

производства регулярных обновлений антивирусного программного обеспечения; обращения внимания при авторизации на доменное имя интернет-ресурса (может произойти подмена имени сайта), в результате чего могут быть скомпрометированы логин, пароль и иные критически важные данные пользователя;

отключения общего доступа и использования надежного пароля для доступа к Wi-Fi точке;

деактивирования автоматического подключения своих устройств к открытым Wi-Fi точкам;

осуществления проверки на наличие чужих (не доверенных) устройств в списке подключенных клиентов на роутере.

Не рекомендуется переходить по непроверенным ссылкам и посещать сайты сомнительного содержания; открывать всплывающие окна, рекламные баннеры и устанавливать предлагаемое неизвестными сайтами программное обеспечение; вводить свой логин и пароль доступа к учетной записи (странице) или системе дистанционного банковского обслуживания при подключении к бесплатным (открытым) точкам Wi-Fi в кафе, транспорте, торговых центрах и т. д.

Использование социальных сетей и мессенджеров подразумевает под собой необходимость:

целесообразно скрывать персональную и контактную информацию о себе (номер телефона, адрес электронной почты, цифровое фото и другие сведения)

в открытом доступе (аккаунт в социальной сети рекомендуется сделать закрытым);

обмениваться сообщениями в социальных сетях и мессенджерах только полностью удостоверившись в личности собеседника, не реагируя на сомнительные просьбы и предложения.

Не рекомендуется использовать указание геолокации на фото и постах; размещать в сети Интернет объявления с указанием используемых номеров телефонов, а также указывать контактные данные мессенджеров (в случае размещения – удалять сразу по миновании надобности).

Безопасность мобильных устройств осуществляется за счет:

использования пин-кода, а также дополнительных способов блокирования устройства (графический ключ, пароль и др.);

своевременного обновления операционной системы устройства, антивирусного и иного программного обеспечения;

установления приложений только из проверенных источников; обращения внимания, к каким функциям гаджета приложение запрашивает доступ; включения встроенных функций устройства для определения его местонахождения;

незамедлительной смены паролей к интернет-банкингу, электронной почте и другим сервисам в случае утери (хищения) устройства;

обязательного изменения привязки интернет-сервисов к новому номеру (лучше сделать это заблаговременно) при смене абонентского номера;

сброса устройства до заводских настроек при его продаже.

Не рекомендуется передавать незнакомым мобильный телефон или сим-карту (в случае передачи – контролировать все действия, которые производятся с устройством); устанавливать приложения с низким рейтингом и отрицательными отзывами; перезванивать на незнакомые иностранные номера; хранить важную информацию на мобильном устройстве; делать полное снятие ограничений на устройстве.

Получение достоверной информации

В контексте развития и повсеместного использования нейросетевых технологий, способных генерировать фото и видеоконтент о событиях, не происходивших в действительности, а также с использованием изображений лиц, не имеющих отношение к реальности, особую актуальность приобретает умение отличать достоверную информацию от дипфейков. Дипфейк – методика синтеза изображения, основанная на искусственном интеллекте. Методика синтеза изображения используется для соединения и наложения существующих изображений и видео на исходные изображения или видеоролики. Для того чтобы удостовериться в оригинальности информации, необходимо произвести ее верификацию.

Верификацией называют технологию проверки информации на достоверность, правильность, точность. Верификация не обязательно сложна. Для нее не требуется сложных алгоритмов или доступа к продвинутым инструментам или программам, которые автоматически определяли бы, является ли снимок фейком или манипуляцией.

Существует простая инструкция по верификации фотографий и видео, которая поможет в спорных ситуациях. Инструкция из пяти шагов поможет проверить как источник, так и содержание, просто ответьте на вопросы:

1. Имеете ли вы дело с оригиналом?
2. Знаете ли вы, кто сделал фото/видео?
3. Знаете ли вы, где было сделано фото/видео?
4. Знаете ли вы, когда было сделано фото/видео?
5. Знаете ли вы, почему было сделано фото/видео?

Учитывая, что наиболее распространенные виды подлога представляют собой старые видео и фото, которые распространяют в привязке к актуальным событиям и новостям, при проверке важно убедиться, что материал является или оригинальным, т. е. он не публиковался в интернете раньше и не подвергался обработке, или настолько близким к оригиналу, насколько можно найти.

Найти оригинал можно следующими способами:

обратным поиском изображений через Google Image Search или TinEye и др;

проверкой видео через сервисы Data Viewer;

проверкой теней и отражений;

с использованием инструментов анализа изображений, например, Izitru или Forensically, чтобы выявить признаки обработки (лучше всего проверять исходники изображений, а не файлы, найденные в социальных сетях).

В завершение отметим, что низкий уровень цифровой грамотности отдельных слоев населения напрямую коррелирует с возможностью стать жертвой мошенничества и иных посягательств.

В этой связи необходимо кратко резюмировать базовые правила безопасности в контексте цифровой грамотности:

1. Не отвечать на не ожидаемые телефонные звонки с абонентских номеров иностранных государств, в том числе поступающие в мессенджерах.
2. Не переходить по «подозрительным» ссылкам.
3. Использовать различные пароли для различных ресурсов, стараясь самостоятельно либо с использованием программного обеспечения генерировать «сложные» пароли, содержащие символы верхнего и нижнего регистра, цифры, специальные символы.
4. Не использовать при создании пароля своей фамилии, имени, даты рождения и иных общеизвестных символов.
5. Не хранить пароли в общедоступных ресурсах.
6. Не сообщать пароли и персональные данные третьим лицам.
7. Не пользоваться ресурсами теневого сегмента сети Интернет – Даркнетом.
8. Всегда проверять информацию на официальных ресурсах государственных органов, банков и небанковских кредитно-финансовых организаций.

9. Контролировать посещение детьми ресурсов в глобальной компьютерной сети Интернет, в том числе с использованием функции «Родительский контроль».

10. Обучить родственников пожилого возраста особенностям работы в сети Интернет, объяснить им правил безопасности.

11. Использовать двухфакторную аутентификацию или 2FA (метод проверки личности пользователя, при котором два из трех возможных факторов аутентификации объединяются для предоставления доступа к веб-сайту или приложению).

Вопросы для самоконтроля

1. Что такое цифровая грамотность?
2. Какие аспекты цифровой грамотности выделяются?
3. Какие основные способы обеспечения безопасности мобильных устройств существуют?
4. Какие существуют способы сохранить информацию о себе в тайне при использовании мессенджеров?

Список использованных источников:

1. Князькова, В.С. Цифровая грамотность населения Республики Беларусь: курс на повышение / В.С.Князькова // Бизнес. Образование. Экономика : Междунар. науч.-практ. конф., Минск, 2 апреля 2020 г. : сб. ст. : в 2 ч. / редкол.: В.В.Манкевич (гл. ред.) [и др.]. – Минск : Институт бизнеса БГУ, 2020. – Ч. 1. – С. 68–71;

2. Князькова, В.С. Оценка уровня знаний и навыков населения Республики Беларусь в сфере информационной безопасности в условиях перехода к электронной экономике / В.С.Князькова // Цифровая трансформация. – 2018. – № 3. – С. 34–45;

3. Князькова, В.С. Теоретико-методологический подход к дефиниции понятия «цифровая грамотность» / В.С.Князькова // Новая экономика. – 2019. – Т. 74, № 2. – С. 92–97;

4. Симхович, В.А. Цифровая грамотность населения Беларуси: социально-демографические характеристики / В.А.Симхович // Российский научный журнал «Телескоп: журнал социологических и маркетинговых исследований». Т. 12, 2023. – № 4. – С.11–14.