Цифровая грамотность – императив федерального законодательства
Digital literacy - a federal legislation imperative

С.И. Луценко

Эксперт НИИ Корпоративного и проектного управления (г. Москва). Аналитик Института экономический стратегий Отделения общественных наук Российской академии наук.

Соавтор документа «Стратегия развития электросетевого комплекса Российской Федерации».
Автор проекта «Контуры Концепции развития финансового кластера Российской Федерации на долгосрочную перспективу»
E-mail: scorp_ante@rambler.ru

S.I. Lutsenko

Lutsenko Sergej Ivanovich, Expert, The Corporate and Project Management Institute (Moscow), Analyst, Institute for Economic Strategies of the Social Sciences Division of the Russian Academy of Sciences (Moscow).
The co-author of the document «Strategy of development of an electric grid complex of the Russian Federation».
The author of the project «Contours of the Concept of Developing Financial Cluster of the Russian Federation in the Long-Term Period».

В действующем федеральном законодательстве об информации, информационных технологиях не определена важная категория – цифровая грамотность. Автор анализирует роль и значение цифровой грамотности в современных условиях.

The important category - digital literacy is not specified in the acting federal legislation about the information, information technology. The author analyzes a role and value of digital literacy in modern conditions.

Ключевые слова: цифровая грамотность, угрозы, законодательство, интернет, правовая категория
Keywords: digital literacy, threats, the legislation, the internet, a legal category

Указом Президента Российской Федерации была утверждена «Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 гг.» [7], согласно которой были поставлены задачи развития в стране общества знаний, повышения доступности качества товаров и услуг, которые будут произведены по технологиям цифровой экономики. Данный Указ Президента Российской Федерации определяет задачи повышения уровня информированности и цифровой грамотности.

Однако, дефиниция «цифровой грамотности» в действующем федеральном законодательстве, прежде всего, в Федеральном законе «Об информации, информационных технологиях и о защите информации» не определена [8].

Как отмечается в Рекомендации Комитета Министров Совета Европы «О свободе в Интернете» [5], государство разрабатывает для своих пользователей программы развития медиа- и цифровой грамотности в целях обеспечения их способности принимать информированные решения, а также соблюдать права и свободы других лиц. Оно обеспечивает доступ и использование образовательного, культурного, научного, учебного и иного контента.

В Рекомендации Комитета министров Совета Европы «О соблюдении, защите и осуществлении прав детей в цифровой среде» [6] заключается, что государствам

необходимо содействовать развитию цифровой грамотности, в том числе медийной и информационной грамотности, а также обучению в сфере цифрового гражданства, чтобы гарантировать, что дети обладают соответствующими навыками по разумному взаимодействию с цифровой средой и устойчивостью, которая поможет им справиться со смежными рисками. Обучение цифровой грамотности должно быть включено в базовую учебную программу с самого раннего возраста с учетом развивающихся способностей детей.

Цифровую грамотность необходимо эффективно внедрять в условиях, когда дети используют Интернет, особенно в школах и организациях, работающих с детьми и в интересах детей. Государства также должны поощрять и поддерживать цифровую грамотность родителей или лиц, осуществляющих уход за ребенком, через созданные государством и предназначенные для родителей механизмы, которые служат важным средством создания более безопасной и устойчивой цифровой среды для детей и их семей.

В федеральном законодательстве существует правовой пробел в отношении такой важной категории, как цифровая грамотность.

В результате неурегулированности данной категории, граждане РФ могут столкнуться с определенными угрозами – ущербом их экономическим интересам.

По мере глобального развития такого сегмента потребительского рынка, как электронная коммерция, и вовлечения в него все большего числа активных пользователей Интернета (в том числе за счет расширения спектра соответствующих мобильных средств связи и их доступности) стали заметнее проявляться проблемы незнания российскими потребителями своих прав, умело эксплуатируемые в повседневной практике недобросовестными участниками рынка в целях получения максимальной выгоды в ущерб экономическим интересам и законным правам не только самих потребителей, но и добросовестных представителей бизнес-сообщества.

По мере глобального развития электронной коммерции и вовлечения в нее все большего числа активных пользователей сети «Интернет» (в том числе за счет расширения спектра соответствующих мобильных средств связи и их доступности) недобросовестные участники рынка умело эксплуатируют правовую неграмотность потребителей в целях получения максимальной выгоды, что причиняет ущерб экономическим интересам не только самих потребителей, но и добросовестных представителей бизнес-сообщества.

Поэтому назрела необходимость повышения цифровой грамотности потребителей, для того чтобы они могли пользоваться всем спектром Интернет-технологий, умели находить в сети информацию о товарах (работах, услугах), правильно ее оценивали и делали осознанный выбор при совершении покупок в Интернет-магазине, а также владели навыками защиты от виртуальных угроз [2].

Поэтому на современном этапе так важно сделать акцент в информационно-консультативной работе всех уровней национальной системы защиты прав потребителей именно на этом сегменте потребительского рынка.

По данным РОЦИТ, индекс цифровой грамотности россиян в целом в 2016 г. вырос на 6,3% по сравнению с 2015 г. и на данный момент составляет 5,42 пункта по десятибалльной шкале

В этой связи потребителям необходимо повышать цифровую грамотность, под которой подразумевается умение пользоваться всем спектром интернет-технологий, куда входит не только умение сделать покупку в интернет-магазине, но и умение искать информацию, правильно ее оценивать. Кроме того, очень важны знание базовых алгоритмов правовой защиты своих потребительских прав и навыки защиты от интернет-угроз.

Пользуясь интернет-банкингом, делая покупки в онлайн-магазинах, потребитель рискует потерять свои личные сбережения или передать третьим лицам персональные данные. Поэтому важно довести до пользователей не только тот объем информации,

который предусмотрен потребительским законодательством, но и предупредить их о действиях сетевых мошенников, например, использующих фишинг (электронное письмо, маскирующееся под официальное письмо от банка или известного онлайн-магазина), и тем самым минимизировать риски, связанные с материальными потерями потребителей.

Ключевой проблемой является цифровая грамотность людей пожилого возраста, пенсионеров, которая на сегодняшний день явно недостаточна. Современная жизнь требует цифровой компетентности даже от тех, кто активную часть своей жизни уже прожил. Новые сервисы коммерческих и государственных структур разрабатываются как цифровые «по умолчанию». Особенно это заметно в сфере различных услуг связи, в первую очередь мобильной, активными пользователями которой в последние годы являются люди пожилого возраста. Поэтому необходимо повысить осведомленность пожилой аудитории о преимуществах цифровых знаний и цифровых сервисов. Проще говоря, сделать погружение в цифровую среду привлекательным и полезным для пенсионеров.

Таким образом, цифровая компетентность - это не просто вопрос использования IT-технологий, а общесоциальная проблема [1].

Интересным представляется опыт Республики Казахстан, где в Законе «Об информатизации» [3] сформулирована правовая категория - цифровая грамотность.

Цифровая грамотность - знание и умение человека использовать информационно-коммуникационные технологии в повседневной и профессиональной деятельности.

Кроме того, Законом Республики Казахстан определено, что основными задачами государственного управления в сфере информатизации являются, в числе прочих, повышение цифровой грамотности.

В основе повышения цифровой грамотности лежит создание «креативного общества» - развитие компетенций и навыков для цифровой экономики, подготовка ИКТ специалистов для отраслей.

В настоящее время, количество абонентских устройств, подключенных к интернету, увеличивается и большинство пользователей продолжает игнорировать меры «цифровой гигиены» в отношении себя и принадлежащих им устройств, концепция «Интернета вещей» только усиливает проблему их безопасного использования [4].

Речь идет о традиционных электронных устройствах (персональные компьютеры и ноутбуки), которые имеют возможности по установке и обновлению антивирусного программного обеспечения, то пользователи «Интернета вещей», часто даже не знают, как обезопасить их функционирование.

Такие устройства пока, в принципе, создаются без учета технологических рисков, что делает их потенциальными элементами вредоносных сетей, («ботнет»), используемых для осуществления различных сетевых атак, направленных на потерю доступности информационных систем и влекущих для добросовестных пользователей отказ в обслуживании при оказании информационно - коммуникационных услуг.

Пренебрежение соображениями безопасности при использовании Интернет-ресурсов и социальных сетей ведет к повышенному риску для неприкосновенности частной жизни, несанкционированному использованию или модификации общедоступных персональных данных, а также разглашению персональных данных ограниченного доступа или их экстерриториальной доступности для преступных сообществ или разведывательных структур при их хранении на территории других государств.

Низкая правовая грамотность по вопросам информационной безопасности и отсутствие сформировавшихся потребностей в повышении у населения создают питательную почву для развития правонарушений и преступлений в информационной сфере.

Отсутствие знаний о правовых ограничениях создает иллюзию дозволенности действий, нарушающих права и свободы других граждан, права обладателей авторских и

смежных прав на программное обеспечение и влияющих на функционирование информационных ресурсов.

Тем самым, низкий уровень цифровой грамотности конечных пользователей в вопросах защиты персональных данных при отсутствии базовых знаний по общим методам распространения вредоносных компьютерных программ и программных продуктов (особенно «фишинговые» страницы поддельных интернет-магазинов и банков, распространение вирусных и «троянских» программ через «взломанные» сайты, скачивание нелицензионного («пиратского») программного обеспечения) приводят к тысячам случаев, когда граждане Российской Федерации становятся жертвами, а принадлежащие им технические средства орудиями противоправного использования ИКТ.

Недостаточная осведомленность в методах защиты информации и низкая обеспеченность в системах информационной безопасности предприятий малого и среднего бизнеса, в том числе занятых в сфере оказания информационно - коммуникационных услуг, которые зачастую даже не могут оценить состояние принадлежащей информационно - коммуникационной инфраструктуры, приводят к большому количеству не анализируемых событий и инцидентов информационной безопасности, затрудняющих как профилактику технологических уязвимостей, так и борьбу с преступниками, использующими ИКТ как средство для совершения преступлений.

При этом некоторые страны придерживаются понятия информационной безопасности применительно ко всем аспектам использования ИКТ, выстраивая соответствующую модель правового регулирования и системы государственного управления.

Например, стратегия Норвегии отмечает, что новые услуги и устройства предъявляют весьма высокие требования к компетенции простых пользователей. Но главная ответственность за обеспечение безопасности информации, систем и сетей возлагается на владельца или оператора. Такие работы должны быть частью ежедневной работы и финансироваться наряду с текущими операциями. Стоимость мер по содействию информационной безопасности должна быть соразмерна оценке риска в отдельных сферах управления (глобальный индекс кибербезопасности составляет 0,735).

В основе стратегии Финляндии лежит понимание кибербезопасности как проблемы экономического характера, тесно связанной с развитием финского информационного общества (глобальный индекс кибербезопасности составляет 0,618).

Словакией обеспечение информационной безопасности рассматривается в качестве необходимого условия нормального функционирования и развития общества. Поэтому цель стратегии - служить прочным фундаментом для защиты информации. Стратегия направлена как на предотвращение угроз, так и на обеспечение готовности и устойчивости средств их предотвращения (глобальный индекс кибербезопасности составляет 0,618).

Франция ориентируется на то, чтобы информационные системы были способны противостоять событиям, которые могут отрицательно повлиять на доступность, целостность и конфиденциальность информации, делает упор на технические средства защиты информации, борьбу с киберпреступностью и установлением киберзащиты (глобальный индекс кибербезопасности составляет 0,588).

Стратегия Германии закладывает основу для безопасности критически важных информационных систем. Германия сосредоточена на предотвращении и уголовном преследовании кибератак, а также выхода из строя IT-оборудования, вызванного случайными факторами. Стратегия кибербезопасности Германии определяет уровень кибербезопасности, достигнутый суммой всех национальных и международных мер, принятых для защиты и доступа к информации и коммуникациям, целостности, достоверности и конфиденциальности данных в киберпространстве, а также укреплением германского технологического суверенитета и экономического потенциала во всем

диапазоне основных стратегических IT-компетенций (глобальный индекс кибербезопасности составляет 0,706).

Стратегия безопасности ИКТ Австрии заключается в распространении интегральных подходов к безопасности, реализованных в системе «электронного правительства», к другим областям, включая те, которые должны быть созданы на транснациональном уровне в целях обеспечения долгосрочной жизнеспособности экономики Австрии (глобальный индекс кибербезопасности составляет 0,676).

Подход Великобритании направлен на развитие кибербезопасности. Цель: вывести Соединенное Королевство на первое место по инновациям, инвестициям и качеству сервисов в сфере информационно - телекоммуникационных технологий, и тем самым, в полной мере воспользоваться всеми преимуществами и достоинствами киберпространства. Необходимо исключить риски типа кибератак преступников, террористов и других государств с целью сделать киберпространство безопасным для граждан и экономики (глобальный индекс кибербезопасности составляет 0,706).

Национальная стратегия Швейцарии отмечает необходимость уменьшения влияния преобладающих интересов нескольких стран, участвующих в Интернет-индустрии, рассматривает применение описываемых в ней мер «в мирное время, и тем самым, явным образом исключает войны».

Невозможно учесть всех обстоятельств, связанных с инцидентами в отношении информационной безопасности, но путем осознанного ответственного поведения, прежде всего, со стороны государства (закрепления в федеральном законодательстве положений о цифровой грамотности) допустимо снизить их частоту (внедрение «цифровой гигиены») и защитить населения от ущерба их экономическим интересам.

Литература

1. Государственный доклад Роспотребнадзора «Защита прав потребителей в Российской Федерации в 2016 году» // Федеральная служба по надзору в сфере защиты прав потребителей и благополучия человека. 2017.
2. Государственный доклад Роспотребнадзора «Защита прав потребителей в Российской Федерации в 2017 году» // Федеральная служба по надзору в сфере защиты прав потребителей и благополучия человека. 2018.
3. Закон Республики Казахстан от 24.11.2015 № 418-5 «Об информатизации» // Доступ из СПС «Консультант Плюс».
4. Постановление Правительства от 30.06.2017 № 407 «Об утверждении Концепции кибербезопасности («Киберщит Казахстан») // Доступ из СПС «Консультант Плюс».
5. Рекомендация № CM/Rec(2016)5 Комитета Министров Совета Европы «О свободе в Интернете» (Принята 13.04.2016 на 1253-ом заседании заместителей министров) // Доступ из СПС «Консультант Плюс».
6. Рекомендация № CM/Rec(2018)7 Комитета министров Совета Европы «О соблюдении, защите и осуществлении прав детей в цифровой среде» (Принята 04.07.2018 на 1321-ом заседании представителей министров) // Бюллетень Европейского суда по правам человека. Российское издание. 2018. № 12.
7. Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» // Собрание законодательства РФ. 2017. № 20.
8. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. 2006. № 31 (1 ч.).