БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2023. – № 1 (108). – 36–52

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ

УДК 004.58 DOI: 10.17212/2782-2230-2023-1-36-52

ВОПРОСЫ ЛИЧНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ЭКОНОМИКИ, УПРАВЛЕНИЯ И ОБЩЕСТВЕННЫХ КОММУНИКАЦИЙ*

М.Е. БОЧАРНИКОВА[1], Т.М. ПЕСТУНОВА[2], В.В. СЕЛИФАНОВ[3]

[1] *630090, РФ, Новосибирская область, г. Новосибирск, ул. Пирогова, 2, Новосибирский государственный университет, ассистент кафедры компьютерных систем. E-mail: m.bocharnikova@g.nsu.ru*
[2] *630090, РФ, Новосибирская область, г. Новосибирск, ул. Пирогова, 2, Новосибирский государственный университет, кандидат технических наук, доцент кафедры компьютерных систем. E-mail: t.pestunova@g.nsu.ru*
[3] *630087, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, старший преподаватель кафедры защиты информации. E-mail: sfo1@mail.ru*

В статье дается анализ основных аспектов личной информационной безопасности, знание которых важно для человека в условиях высоких темпов цифровизации социальной и экономической сферы. Они направлены на формирование персонального информационного цифрового пространства и управление им в условиях изменяющихся технологий и правового поля в соответствии с частными и деловыми интересами личности. Первой задачей при этом является осознание человеком своих интересов и потребностей в использовании цифровой среды, а также оценка значимости вопросов безопасности своих персональных данных. Далее обращается внимание на выработку навыков анализа и оценки интернет-ресурсов в контексте достоверности и целей распространения информации, освоение доступных в рамках действующего законодательства методов и средств управления своими персональными данными. Рассмотрены примеры ряда других актуальных задач, существующие возможности практического получения знаний и формирования навыков безопасной работы в цифровой среде для различных категорий пользователей на современном уровне развития информационных технологий, а также обозначены те аспекты, которые пока остаются за рамками методов и технологий, массово используемых для повышения уровня цифровой грамотности населения.

Ключевые слова: информационная безопасность, защита информации, цифровая грамотность, персональные данные, цифровая экономика

* Статья получена 16 февраля 2023 г.

ВВЕДЕНИЕ

Цифровизация экономической и социальной сферы вовлекает в орбиту информационных технологий огромное число пользователей, поскольку одним из краеугольных принципов цифровой экономики является персонализация товаров и услуг. Современный человек всё бóльшую часть жизненных потребностей удовлетворяет посредством цифрового потребления с применением электронной информации и цифровых сервисов для достижения личных целей, решения образовательных или производственных задач. В этих условиях растут риски информационной безопасности (далее – ИБ), вызванные ошибками, легкомыслием, небрежностью и недостаточной цифровой грамотностью людей при работе с многочисленными электронными сервисами, а также действиями злоумышленников, направленными против них, ради получения выгоды. Реализация этих рисков может приводить и уже приводит к ощутимому ущербу как для конкретных людей, так и для организаций, где они работают. Угрозы в информационной сфере, с одной стороны, могут иметь нарушения значимых для деятельности человека качеств информации (конфиденциальность, целостность, доступность и др.), а с другой – навязывать человеку некую информацию с целью формирования такой модели его поведения, при которой он будет совершать действия в интересах третьих лиц, даже не понимая этого. В результате осознания этих рисков в последние годы многократно возросло внимание к проблеме персональной (личной) ИБ как со стороны государства, так и со стороны отдельных отраслей. Так, в число основных направлений в Доктрине информационной безопасности входит «обеспечение защищенности граждан от информационных угроз, в том числе за счет формирования культуры личной информационной безопасности» [1]. Одной из задач национальной программы развития цифровой экономики России является повышение цифровой грамотности населения, что включает и вопросы цифровой безопасности. В статье дается анализ основных аспектов персональной ИБ, изучение которых важно для различных категорий пользователей для снижения негативных последствий от реализации информационных рисков в условиях

1. ЦЕЛИ И ЗАДАЧИ ЛИЧНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Реализация принципа персонализации приводит к накоплению и обработке в глобальной цифровой среде огромных объемов разнообразных данных, которые либо являются *персональными данными* (далее – ПД), либо могут ими стать спустя какое-то время, часто их называют «социальные данные».

На правовом уровне регулирование этих процессов осуществляется посредством законодательства о ПД, целью которого является «обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну» [2]. Достижение целей закона обеспечивается, с одной стороны, предъявлением к организациям-операторам требований о целенаправленности и законности обработки ПД, их актуальности и безызбыточности по отношению к заявленным целям, обеспечению их безопасности. В любом случае необходимо получение согласия субъекта на обработку его ПД (за исключением ряда случаев, прямо указанных в законе). А с другой стороны, субъект ПД имеет право получать от оператора сведения об обработке своих ПД (в том числе о содержании ПД, целях и способах обработки, мерах безопасности), требовать обеспечения актуальности обрабатываемых данных и по желанию отзывать данное ранее согласие на обработку ПД.

Цифровизация бизнес-процессов и концентрация ПД в электронной среде таит немало «подводных камней», которые могут привести к нарушению интересов и прав субъекта ПД, обостряя противоречия между ним и операторами, собирающими и обрабатывающими ПД. Эти противоречия – следствие того, что оператор для повышения эффективности бизнес-процессов стремится расширить состав используемых ПД сверх того, что нужно для целей, установленных в согласии на обработку. Таким образом, цели обработки ПД для субъекта и оператора перестают совпадать.

Данные о личности в цифровой среде, которые могут обрабатываться оператором, можно разделить на три основные группы. Первая группа – первичные данные – это те данные, которые человек предоставляет оператору и на обработку которых он дает согласие. Вторая группа – назовем их дополнительными данными – это данные, которые оператор накапливает в процессе использования человеком соответствующих электронных сервисов (сведения о платежных транзакциях, телефонных звонках, приобретении товаров и услуг и т. п.). Обработка данных, типовых для конкретного электронного бизнеса, также может быть учтена в согласии, однако по мере цифровизации их содержание может существенно расшириться, а цель использования может оказаться совсем не той, которая заявлена при получении согласия. Третья группа – данные о человеке, которые оператор может получить из общедоступных источников (например, из соцсетей, личных страниц на интернет-ресурсах и т. д.) – социальные данные. Даже если эти данные используются для законных целей и получены легитимным путем, то достоверность и актуальность их отнюдь не гарантированы, а следовательно, не гарантирована и корректность решений, принятых на их основе. Важно заметить, что в действующей редакции закона о персональных данных имеются положения,

помогающие человеку регулировать распространение своих персональных данных, размещенных по его желанию на общедоступных ресурсах. Определена особая категория – «персональные данные, разрешенные субъектом персональных данных для распространения» [2], на обработку которых каждый заинтересованный в этом оператор должен получить отдельное согласие субъекта ПД, однако далеко не все люди знают об этих возможностях и о том, как их реализовать. Одной из наиболее критичных для субъекта ПД является ситуация, когда для сбора и обработки указанных данных используются формальные алгоритмы (в том числе интернет-роботы, нейросети и другие средства искусственного интеллекта), и исключительно на основе результатов такого анализа в отношении человека принимаются решения, имеющие юридические, финансовые и другие последствия для него. При этом подобные решения могут быть исполнены автоматически в информационной системе (без участия сотрудника оператора). Человек же узнает об этом только постфактум, когда, например, обнаружит блокирование своего банковского счета или невозможность выезда за границу из-за долга своего тезки-однофамильца, получит отказ в трудоустройстве от работодателя или в получении кредита в банке из-за фейковой информации в соцсетях. Поток такого рода примеров нарастает очень быстрыми темпами. Законодательство и практика его применения явно не успевает за развитием цифровых технологий. В погоне за цифровизацией новых сфер государство и бизнес не спешат исправлять даже регулярно появляющиеся и признанные проблемы. Проблема «тезок-однофамильцев» – один из ярких примеров, решить который можно было бы установлением адекватных требований к минимально необходимой информации для идентификации человека как в государственных, так и в иных информационных системах, а до этого времени – как минимум упрощением процедур «восстановления правды» и отменой автоматических действий, которые могут нанести существенный ущерб человеку. Проблема соотнесения личности человека с его цифровым образом, на основании которого в отношении него принимаются те или иные решения, становится серьезной проблемой обеспечения защиты прав субъекта ПД в цифровой реальности.

Актуальный подход в защите данных о личности в цифровой среде основан на тезисе о том, что данные в цифровой среде принадлежат тому, о ком эти данные. Он изложен в Общем регламенте защиты данных (General Data Protection Rools, GDPR), развивающем положения Конвенции СЕ № 108 о защите данных с учетом процессов цифровизации. Но и в условиях действующей правовой базы в сфере ПД многое (хотя, безусловно, далеко не всё!) зависит от степени понимания человеком значимости этой проблемы, его желания и ответственного отношения к управлению своими ПД и связанной с ними информацией в цифровой среде. Знание правовых основ защиты ПД,

понимание рисков организации бизнес-процессов в цифровой среде, умение работать с соблюдением основных правил ИБ при применении электронных сервисов могут существенно снизить вероятность попадания в ситуации, чреватые ущербом от использования цифровых технологий.

Исходя из сказанного, в условиях цифровой трансформации экономической и социально-культурной сферы можно сформулировать *цель личной ИБ – формирование на основе частных и деловых интересов персонального информационного цифрового пространства и управление им в условиях изменяющихся информационных технологий и правового поля.*

Отправной точкой для достижения поставленной цели является *задача осознания человеком своих интересов и потребностей в использовании цифровой среды, а также необходимых аспектов безопасности своих ПД* как основы при принятии решений об их предоставлении и распространении в цифровом пространстве. Для этого необходимо научиться соотносить цель, объем, условия и способы обработки ПД операторами с собственными потребностями и интересами использования цифровых сервисов (профессиональными, образовательными и др.). Формирование персонального информационного цифрового пространства основано, с одной стороны, на желании человека решать свои задачи и осуществлять коммуникации с использованием новых информационных технологий, с другой – на умении поиска сервисов, обеспечивающих реализацию тех или иных его потребностей, а в-третьих – на понимании рисков ПД, обусловленных выбранным набором ресурсов и сервисов. В частности, особо внимательно надо относиться к применению широко рекламируемых ныне сервисов, требующих предоставления биометрических данных. Информационные сервисы, используемые для решения задач, связанных с частной жизнью (управление финансами, покупка товаров, госуслуги, образование, билеты, новостной интернет-серфинг, соцсети и другие сервисы для общения и развлечения), развиваются очень быстро, высокими темпами растет и количество их пользователей. Заметим, что пандемия COVID-19 стала мощным «ускорителем» этих процессов. Но в условиях, когда далеко не все разработчики придерживаются практик безопасного программирования, это приводит к росту уязвимого ПО и связанных с ними кибератак. А массовый переход сотрудников на дистанционную работу существенно повышает и риски корпоративным информационным ресурсам из-за того, что пользователи не всегда следуют требованиям корпоративных политик безопасности, работая за пределами офиса. Эффективный поиск, выбор и безопасное использование информационных сервисов в профессиональной деятельности и для обеспечения своих частных интересов – один из важнейших навыков для современного человека.

Вторая ключевая задача при формировании личного информационного пространства – научиться анализировать и оценивать интернет-ресурсы в контексте достоверности и целей распространения информации. События последнего года наглядно продемонстрировали всем людям, насколько жесткой может быть «фейковая война» и каковы ее возможности по навязыванию обществу представлений о происходящих событиях на основе псевдофактов. Но опасность попасть на уловки мошенников высока и в обычной жизни, что требует не только знаний, но ряда важных умений и навыков, касающихся выявления фишинговых и других небезопасных сайтов, противодействовия агрессивной таргетированной рекламе, оценки источников и достоверности представленной информации.

Третья важная задача состоит в освоении доступных в рамках действующего законодательства методов и средств управления своими персональными данными. Закон о ПД в целом предоставляет человеку немалые возможности в этом направлении, однако большинство пользователей слабо знакомы с ними и в еще меньшей степени готовы ими пользоваться. Например, нередко складывается ситуация, когда операторы включают в согласие об обработке ПД большое количество необязательных данных (например, в своих маркетинговых целях), а человек не решается их вычеркнуть из своего согласия или хотя бы поинтересоваться у оператора, зачем именно эти данные нужны, ограничиваясь последующим высказыванием недовольства в частных разговорах с коллегами и друзьями. Пользователи далеко не всегда обращают внимание на мелкий шрифт в электронных формах с текстом о согласии на получение рекламной информации и услужливо проставленной «галочкой», которую можно просто убрать, чтобы избежать ненужных писем, звонков и SMS. Еще реже пользуются правом отказа от обработки ПД после того, как их предоставили. Имеющийся личный опыт показывает, что решение многих вопросов не требует больших усилий, но человеку важно знать свои права и порядок их реализации, а также существующие уже сейчас способы и инструменты управления ПД, в том числе возможность ограничить распространение и использование своих данных. Эта задача согласуется с задачей проекта «Информационная безопасность» в национальной программе «Цифровая экономика РФ» [3] – обеспечить «контроль обработки и доступа к персональным, большим пользовательским данным, в том числе в социальных сетях и прочих средствах социальной коммуникации, а также возможность отзыва или уменьшения объема ранее данного согласия на обработку персональных данных».

Четверная входящая в сферу личной ИБ задача – освоение практических навыков безопасной работы при использовании цифровых технологий. Удобство и безопасность часто находятся на разных чашах весов при выборе и ис-

пользовании информационных технологий. Пользователи далеко не всегда в достаточно полной мере знают о существующих информационных рисках, а между тем социальная инженерия вкупе с вредоносным программным обеспечением стабильно занимает лидирующие позиции в статистике атак на информационные системы. Вопросы ИБ не всегда изучаются в качестве отдельных дисциплин в вузах, а часто входят обзорно в другие курсы (например, в информатику), где их можно осветить лишь обзорно [4], что недостаточно для формирования умений и навыков по безопасной работе в цифровой среде. С точки зрения актуальных угроз и способов обеспечения личной ИБ следует обратить внимание на обучение по следующим аспектам. *Аутентификационная информация* является одним из основных объектов атак, поэтому пользователи при использовании любых информационных технологий должны уметь обеспечить надежность и защищенность своей аутентификации (создание сложных паролей, конфиденциальность при хранении и передаче по сети, своевременная замена, конфиденциальность ключевой и парольной информации при использовании съемных электронных носителей – смарт-карт, токенов и др.). *Социальная инженерия* (фишинг: почтовый, телефонный, SMS, интернет) является доминирующим видом атак на пользователей, поэтому умение оперативно определить эту угрозу и правильно отреагировать («не клюнуть на удочку») – насущная потребность для всех пользователей и при работе в корпоративных информационных системах, и при использовании информационных технологий в личных целях. *Вредоносное программное обеспечение* – еще одна давняя, но не теряющая с годами своей актуальности угроза, уметь противодействовать которой должен каждый пользователь. Установка антивируса является началом этой работы, но далее важно не забывать о его правильной настройке, обновлении баз и других деталях (например, о том, что файл, открытый на «недопроверенной» антивирусом «флэшке», вполне может стать источником заражения компьютера), уметь обращать внимание и правильно реагировать на признаки возможных заражений. Следующий обширный блок – *правила безопасной работы с интернет-ресурсами*. Пользователь должен различать безопасное и небезопасное соединение, понимать риски «бездумного» перехода по ссылкам, проявлять осторожность при скачивании информации с интернет-ресурсов, контролировать следующее: безопасность при работе с сайтами, содержащими регистрационные сервисы, особенности угроз и обеспечения безопасности при работе с электронной почтой и в соцсетях, правила безопасности при совершении электронных финансовых операций, риски использования облачных сервисов. Работая на персональном компьютере, надо уметь настраивать основные функции безопасности браузеров, понимать уязвимости полезных на первый взгляд функций (например, автозаполнение полей и сохранение паролей),

настраивать параметры встроенных инструментов безопасности в соответствии со своими потребностями, а также обеспечить безопасность домашнего подключения к сети.

Поскольку одними из самых распространенных устройств доступа в интернет являются смартфоны и другие мобильные устройства, то *безопасность при работе с ними* – еще одна важная тема в личной информационной безопасности. Она имеет много общего с рассмотренной выше проблематикой интернет-безопасности, но есть немало специфических угроз и уязвимостей, характерных именно для мобильных устройств. В частности, в случае утраты устройства уметь избежать ущерба из-за случайного разглашения персональных данных или не допустить такой утечки при желании избавиться от надоевшего устройства (продать, подарить, выбросить), понимать риски неконтролируемого использования видеокамер, диктофонов, геолокации и других встроенных сервисов.

С развитием юридически значимого электронного документооборота и отказом от электронных оригиналов документов во многих сферах деятельности особое значение для пользователей приобретают *навыки обеспечения безопасности при применении электронной подписи*. Они должны иметь представление о принципах функционирования таких технологий и их уязвимостях, знать установленные законодательством виды электронных подписей и понимать, с какими из них они реально работают, знать соответствующие правила безопасности, а также условия признания подписанных электронных документов равнозначными документами на бумажном носителе с собственноручной подписью.

В целях *управления своими персональными данными* пользователю необходимо знать правовые аспекты этой сферы и электронные сервисы взаимодействия с операторами и уполномоченным органом по защите прав субъектов персональных данных, возможности ознакомления со своими ПД и контроля законности их обработки, особенности заполнения и отзыва согласия на обработку ПД (в том числе согласие на обработку ПД, разрешенных для распространения) и т. п.

«Нестареющими» важными темами являются обеспечение *доступности и целостности информации, методы ее резервирования и восстановления.*

С учетом высоких темпов изменчивости цифровой среды проблематика личной информационной безопасности не стоит на месте и постоянно расширяется, охватывая вопросы безопасности, присущие качественно новым информационным технологиям, которые уже стали достаточно массовыми или станут таковыми в ближайшей перспективе. К подобным технологическим новациям можно отнести интернет вещей, умный дом, блокчейн, многочисленные цифровые сервисы на основе искусственного интеллекта, беспилот-

ные аппараты, устройства-роботы и многое другое. Так, в частности, *в последние годы новые актуальные проблемы ИБ обусловлены быстрым развитием интернета вещей,* или, как принято называть, устройств IoT [7–12]. Компании внедряют их для автоматизации сбора информации и управления различными сферами своей деятельности. Может использоваться совокупность устройств, которые объединены концепцией сети передачи данных. Часто объединение происходит с использованием Bluetooth, wi-fi и других беспроводных технологий. Причем это могут быть как бытовые устройства (лампочки, выключатели, кофе-машины, кулеры, печки и т. д.), так и персональные компьютеры, телефоны, которые находятся в критически уязвимом состоянии, если у них общая система с бытовыми IoT-устройствами. И, как правило, такого рода устройства очень уязвимы. Более того, встречаются такие уязвимости, которые могли быть устранены на персональном компьютере с десяток лет назад. В отсутствие должного контроля над IoT-системами компании не могут гарантировать сохранность ПДн. И в частной жизни всё чаще люди используют IoT для широкого спектра целей – от организации «умного дома» до мониторинга своих физиологических параметров. Для бытовых приборов унифицированных требований ИБ практически не существует, и в целом регулирование вопросов безопасности IoT находится на начальном этапе. Хотя была разработана и утверждена концепция построения и развития узкополосных беспроводных сетей связи интернета вещей [9], где прописаны некоторые стандарты создания и управления устройствами IoT, в том числе рекомендации по ИБ, а создатели устройств предлагают собственные концепции их безопасности (не всегда открытые для изучения), этого безусловно недостаточно. В отсутствие действенной системы регулирования интернета вещей повышение осведомленности пользователей IoT об информационных рисках, связанных с этими устройствам, имеет особое значение. И, размышляя о приобретении (например, об «умной кровати»), человек должен думать не только о том, сколько многообещающих для улучшения сна сервисов описано в рекламе, но и об уровне риска для своего здоровья, если в функционирование соответствующего ПО (в клиентском приложении на смартфоне пользователя или в непонятно где размещенной серверной части) вмешается вредоносная программа или злоумышленник. А надевая на руки «умные часы», не следует забывать и возможных последствиях их уязвимостей – ведь, например, получив данные колебаний акселерометра, особенно в сочетании с графиками гироскопа, можно считать специфический поведенческий профиль пользователя, вплоть до расшифровки пин-кода банковской карты по характерным колебаниям руки [11, 12].

Превентивное ознакомление с уязвимостями новых технологий позволит людям более грамотно подходить к их применению, учитывая требования безопасности уже на этапе их освоения.

2. ПРАКТИЧЕСКИЕ АСПЕКТЫ ПОЛУЧЕНИЯ ЗНАНИЙ И ФОРМИРОВАНИЯ НАВЫКОВ ПО ОБЕСПЕЧЕНИЮ ПЕРСОНАЛЬНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Приобретение знаний и умений обеспечения личной ИБ может осуществляться разными способами. В целом, активное развитие электронных услуг на фоне часто появляющейся в СМИ информации об утечках персональных данных и последствиях инцидентов информационной безопасности, происходящих в том числе из-за неграмотности и беспечности пользователей, способствует осознанию гражданами важности данной проблемы и повышению их интереса к освоению навыков личной ИБ. Так, многие пользователи знакомятся с базовыми правилами обеспечения интернет-безопасности при регистрации в сервисах интернет-банкинга, при использовании электронных государственных услуг – в основном это касается безопасности аутентификационной информации.

Представители органов власти, государственных организаций и предприятий оборонного комплекса обязаны проходить повышение квалификации по ИБ в соответствии с требованиями законодательства. Круг изучаемых вопросов в первую очередь охватывает правила безопасной работы в информационных системах организации, в том числе в государственных информационных системах, на объектах критической информационной инфраструктуры и в информационных системах персональных данных (с акцентом на обязанности обучаемых сотрудников). Полученные при этом знания во многом универсальны и безусловно способствуют формированию необходимых навыков безопасной работы пользователя с информационными технологиями и за пределами корпоративной информационной среды.

В последние годы стало уделяться значительное внимание вопросам информационной безопасности и защиты персональных данных детей. Эта тематика включается в программы среднего образования, а первые знания школьники могут получить уже в начальных классах [13, 14].

В системе высшего и среднего профессионального образования обучающимся даются представления об используемых в профессиональной сфере информационных системах и технологиях. В стандартах большинства направлений высшего образования предусмотрены компетенции, направленные на формирование способности применять их с учетом требований информаци-

онной безопасности. Однако, как показывает опыт, вопросы личной информационной безопасности в силу ограниченности учебного времени в вузах изучаются, как правило, фрагментарно: обучающих обычно знакомят с отдельными аспектами ИТ-безопасности, но вопросы, относящиеся, например, к обеспечению прав субъектов ПД, практически не затрагиваются.

Как и во многих областях знаний, эффективным способом освоения рассматриваемой проблематики являются семинары и деловые игры с применением активных форм обучения на основе сценариев, адаптированных к интересам аудитории. Для этой цели полезно использовать предварительное анкетирование слушателей, сформулировав задачи ИБ в контексте ситуаций, типичных или достаточно реальных для собравшейся аудитории. Анкеты могут заполняться анонимно, в электронной или письменной форме. Анкетирование позволяет выявить наиболее востребованные аспекты и пробелы в знаниях, что дает возможность настройки обсуждения на аудиторию. Коллективное обсуждение проблемных ситуаций, отраженных в анкетах, активизирует аудиторию и позволяет выйти на реальные примеры, с которыми сталкивались пользователи, что способствует усвоению способов безопасного поведения и предотвращения небезопасных действий в будущем. Заметим, что на некоторые вопросы анкеты может не быть однозначно правильных ответов (например, есть разные относительно безопасные способы создания и хранения паролей), пользователям надо понимать достоинства и риски, связанные с каждым из них.

Интерес обучающихся к обсуждаемой тематике можно поддерживать за счет использования инфографики, анимированных электронных ресурсов, где разбираются типичные ситуации в занимательной форме. Примером могут служить материалы, размещенные на ресурсах по безопасности пользователей в сети интернет [17] и цифровой грамотности [18]. Нередко публикуются образовательные анкеты-тесты, в которых в изображенной и (или) словесно описанной ситуации требуется выбрать правильный с точки зрения безопасности вариант действий, при этом после совершения выбора открываются необходимые комментарии, поясняющие правильный выбор. Не подвергая сомнению полезность и востребованность таких ресурсов, следует отметить, что, просматривая анимации и комиксы, человек часто не ассоциирует свои ИТ-потребности с ситуациями вокруг виртуальных персонажей, поэтому задача заключается в использовании их таким образом, чтобы развлекательная форма представления материалов не затмевала реальных проблем слушателей, и они могли бы представленную тематику сопоставить с собственным опытом применения цифровых технологий. Созданный общедоступный электронный сервис по освоению цифровой грамотности позволяет осуществить самооценку ключевых компетенций цифровой экономики [18], в числе кото-

рых есть и компетенции по информационной безопасности. Однако следует заметить, что в тестах по информационной безопасности на этом ресурсе всё же немало вопросов, которые ориентированы в большей степени на специалистов, а не на пользователей даже при выборе самой самого простого уровня.

Перспективной образовательной технологией в рассматриваемой области является проведение с использованием электронных игровых обучающих платформ квестов, викторин, конкурсов, сценарии которых основаны на реальных ситуациях и требуют от пользователей активного применения своих знаний для достижения целей игры, которая может проводиться в командном или личном формате. Подобные форматы были созданы и сейчас активно развиваются в первую очередь для подготовки специалистов по информационной безопасности. В последние годы на общероссийском и региональном уровнях проводится немало соревнований по ИБ для школьников и студентов, требующих решения практико-ориентированных задач в офлайн- и онлайн-форматах, способствующих пониманию особенностей реализации информационных угроз и выработке навыков их предотвращения [5, 6, 15, 16]. Имеющийся опыт показывает, что при правильном подборе сценариев подобные платформы и форматы мероприятий могут быть интересны и эффективны при повышении осведомленности пользователей в сфере информационной безопасности, обучении их способам противодействия информационным угрозам с применением доступных методов и средств [6].

ЗАКЛЮЧЕНИЕ

В целом, как можно увидеть даже из краткого обзора, в настоящее время пользователям информационных технологий доступно немало возможностей формирования навыков безопасной работы в цифровой среде. Однако этого недостаточно для обеспечения личной информационной безопасности, поскольку основополагающая проблема – формирование персонального цифрового пространства, отвечающего частным и деловым информационным потребностям человека в цифровом мире – требует для своего решения углубленного внимания к вопросам анализа качества информационных ресурсов, сопоставления удобств цифровых сервисов с возможными рисками их использования. Эти аспекты, за редким исключением, пока остаются за рамками методов и технологий, массово используемых для повышения уровня цифровой грамотности населения.

СПИСОК ЛИТЕРАТУРЫ

1. Доктрина информационной безопасности Российской Федерации: утв. Указом Президента РФ от 05.12.2016 № 646 // Собрание законодательства Российской Федерации. – 2016. – № 50. – Ст. 7074.

2. Федеральный закон Российской Федерации от 27 июля 2006 г. № 152 «О персональных данных» // Собрание законодательства Российской Федерации. – 2006. – № 31, ч. 1–2. – Ст. 3448.

3. Паспорт национальной программы «Цифровая экономика Российской Федерации»: утв. президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам 24 декабря 2018 г. № 16.

4. *Тушко Т.А. Пестунова Т.М.* Информатика: учебное пособие. – Красноярск: СФУ, 2017. – 204 с.

5. CTF News: web-сайт. – URL: https://ctfnews.ru/ (дата обращения: 10.03.2023).

6. Концепция CTF-квеста по информационной безопасности для студентов непрофильных специальностей / К.В. Курносов, А.И. Пестунов, Т.М. Пестунова, Я.В. Юракова // Труды Межвузовской научно-практической конференции «Актуальные проблемы обеспечения информационной безопасности». – Самара, 2017. – С. 119–123.

7. Горе от ума: Уязвимости IoT-устройств. – URL: https://vc.ru/tech/150042-gore-ot-uma-uyazvimosti-iot-ustroystv (дата обращения: 10.03.2023).

8. Информационная безопасность в IoT. – URL: https://habr.com/ru/post/700800/ (дата обращения: 10.03.2023).

9. Приказ Минцифры России от 29.03.2019 № 113 «Об утверждении Концепции построения и развития узкополосных беспроводных сетей связи “Интернета вещей” на территории РФ».

10. *Верещагина Е.А., Карпецкий И.О., Ярмонов А.С.* Проблемы безопасности Интернета вещей: учебное пособие. – М.: Мир науки, 2021. – URL: https://izd-mn.com/PDF/20MNNPU21.pdf (дата обращения: 10.03.2023).

11. *Лачынова М.Е.* Аналитическое исследование угроз и уязвимостей умных часов // Социотехнические и гуманитарные аспекты информационной безопасности: материалы III Всероссийской научно-практической конференции. – Пятигорск, 2022. – С. 129–140.

12. Безопасны ли умные часы? // Kaspersky: web-сайт. – URL: https://www.kaspersky.ru/resource-center/threats/smartwatch-security-risks (дата обращения: 10.03.2023).

13. Примерная образовательная программа учебного курса «Информационная безопасность» для образовательных организаций, реализующих про-

граммы начального общего образования (одобрена решение ФУМО от 26 октября 2020 г.). – URL: https://fgosreestr.ru/uploads/files/0f72931702387091b607da108ba104d9.pdf (дата обращения: 10.03.2023).

14. Методические рекомендации по основам информационной безопасности для обучающихся общеобразовательных организаций с учетом информационных, потребительских, технических и коммуникативных аспектов информационной безопасности. – URL: https://единыйурок.рф/images/doc/metod/cyber.pdf (Дата обращения: 10.03.2023).

15. На базе СибГУТИ прошла интеллектуально-патриотическая игра «Киберзарница – 2019». – URL: https://sibsutis.ru/news/2901354/ (дата обращения: 10.03.2023).

16. Школьники региона приняли участие в Кубке Новосибирской области по кибербезопасности // Министерство цифрового развития и связи Новосибирской области. – 2022. – 19 апреля. – URL: https://digit.nso.ru/news/1971 (дата обращения: 10.03.2023).

17. Безопасность пользователей в сети интернет: интернет-портал Национального центра по компьютерным инцидентам. – URL: https://safe-surf.ru/ (дата обращения: 10.03.2023).

18. Готов к цифре. Проект о безопасном и эффективном использовании цифровых технологий для людей с разными уровнями цифровых компетенций. – URL: https://готовкцифре.рф (дата обращения: 10.03.2023).

Бочарникова Андрей Дмитриевич, ассистент кафедры компьютерных систем Новосибирского государственного университета. Область научных интересов – информационная безопасность, компьютерные системы. E-mail: m.bocharnikova@g.nsu.ru

Пестунова Тамара Михайловна, доцент кафедры компьютерных систем Новосибирского государственного университета. Область научных интересов – информационная безопасность, компьютерные системы. E-mail: t.pestunova@g.nsu.ru

Селифанов Валентин Валерьевич, старший преподаватель кафедры защиты информации Новосибирского государственного технического университета. Область научных интересов – информационная безопасность, компьютерные системы. E-mail: sfo1@mail.ru

DOI: 10.17212/2782-2230-2023-1-36-52

Personal information security issues in the context of digital transformation of the economy, management and public communications*

M.E. Bocharnikova[1], T.M. Pestunova[2], V.V. Selifanov[3]

[1] *630090, Russian Federation, Novosibirsk, Pirogov Street 2, Novosibirsk State University, assistant of the Department of Computer Systems. E-mail: m.bocharnikova@g.nsu.ru*
[2] *630090, Russian Federation, Pirogov Street 2, Novosibirsk State University, Candidate. in Technical Sciences, associate professor of Computer Systems Department. E-mail: tmrp54@yandex.ru*
[3] *630087, Russian Federation, Novosibirsk, 20 Karl Marx Prospekt, Novosibirsk State Technical University, senior lecturer of the Department of Information Security. E-mail: sfo1@mail.ru*

The article analyzes the main aspects of personal information security, the knowledge of which is important for a person in conditions of high rates of digitalization of social and economic spheres. They are aimed at the formation of a personal information digital space and its management in the conditions of changing technologies and the legal field in accordance with the private and business interests of the individual. The first task in this case is to make a person aware of their interests and needs in the use of the digital environment, to assess the significance of the issues of the security of their personal data. Further, attention is drawn to the development of skills for analyzing and evaluating Internet resources in the context of the reliability and purposes of information dissemination, the development of methods and means of managing your personal data available within the framework of current legislation. Examples of a number of other relevant tasks, existing opportunities for practical acquisition of knowledge and formation of skills for safe work in a digital environment for various categories of users at the current level of information technology development are considered, and those aspects that remain outside the scope of methods and technologies that are massively used to increase the level of digital literacy of the population are also identified.

Keywords: Information security, information protection, digital literacy, personal data, digital economy, IoT devices, personal information security

REFERENCES

1. Information Security Doctrine of the Russian Federation. Sobranie zakonodatel'stva Rossiiskoi Federatsii = Collection of the legislation of the Russian Federation, 2016, no. 50, art. 7074. (In Russian).

2. Federal Law of the Russian Federation of July 27, 2006 No. 152 "On Personal Data". Sobranie zakonodatel'stva Rossiiskoi Federatsii = Collection of the legislation of the Russian Federation, 2006, no. 31, art. 3448. (In Russian).

* *Received 16 February 2023,*

3. Passport of the national program "Digital Economy of the Russian Federation" (approved by the Presidium of the Council under the President of the Russian Federation for Strategic Development and National Projects on December 24, 2018 No. 16). (In Russian).

4. Tushko T.A. Pestunova T.M. Informatika [Computer Science]. Krasnoyarsk, Siberian Federal University Publ., 2017. 204 p.

5. CTF News: website. (In Russian). Available at: https://ctfnews.ru/ (accessed 10.03.2023).

6. Kurnosov K.V., Pestunov A.I., Pestunova T.M., Yurakova Yu.V. [Concept of CTF-quest on information security for students of non-core specialties]. Trudy Mezhvuzovskoi nauchno-prakticheskoi konferentsii «Aktual'nye problemy obespecheniya informatsionnoi bezopasnosti» [Proceedings of the Interuniversity Scientific and Practical Conference "Actual Problems of Ensuring Information Security"]. Samara, 2017, pp. 119–123. (In Russian).

7. Woe from Wit: Vulnerabilities of IoT devices. (In Russian). Available at: https://vc.ru/tech/150042-gore-ot-uma-uyazvimosti-iot-ustroystv (accessed 10.03.2023).

8. Information security in the IoT. (In Russian). Available at: https://habr.com/ru/post/700800/ (accessed 10.03.2023).

9. Order of the Ministry of Communications of Russia from 29.03.2019 No. 113 "On approval of the Concept of building and development of narrowband wireless communication networks “Internet of Things” on the territory of the Russian Federation". (In Russian).

10. Vereshchagina E.A., Karpetskii I.O., Yarmonov A.S. Problemy bezopasnosti Interneta veshchei [Internet of Things security issues]. Moscow, Mir nauki Publ., 2021. Available at: https://izd-mn.com/PDF/20MNNPU21.pdf (accessed 10.03.2023).

11. Lachynova M.E. [Analytical study of threats and vulnerabilities of smart watches]. Sotsiotekhnicheskie i gumanitarnye aspekty informatsionnoi bezopasnosti [Sociotechnical and Humanitarian Aspects of Information Security]. Materials of the III All-Russian Scientific and Practical Conference. Pyatigorsk, 2022, pp. 129–140. (In Russian).

12. Are smart watches safe? Kaspersky: website. (In Russian). Available at: https://www.kaspersky.ru/resource-center/threats/smartwatch-security-risks (accessed 10.03.2023).

13. Model educational program of the course "Information security" for educational organizations implementing programs of primary general education (approved by the decision of the federal educational and methodological association for general education on October 26, 2020). (In Russian). Available at: https://fgosreestr.ru/uploads/files/0f729317023870 91b607da108ba104d9.pdf. (accessed 10.03.2023).

14. Methodological recommendations on the basics of information security for students of general educational organizations, taking into account information, consumer, technical and communicative aspects of information. (In Russian). Available at: https://единыйурок.рф/images/doc/metod/cyber.pdf (accessed 10.03.2023).

15. SibGUTI hosted an intellectual and patriotic game "Cyberzarnitsa – 2019". (In Russian). Available at: https://sibsutis.ru/news/2901354/ (accessed 10.03.2023).

16. Students of the region took part in the Cup of the Novosibirsk region on cybersecurity. Ministry of Digital Development and Communications of the Novosibirsk Region, 2022, 19 April. (In Russian). Available at: https://digit.nso.ru/news/1971 (accessed 10.03.2023).

17. Security of users on the Internet. National Computer Incident Center Internet Portal. (In Russian). Available at: https://safe-surf.ru/ (accessed 10.03.2023).

18. Ready for digital. A project about the safe and effective use of digital technology for people with different levels of digital competence. (In Russian). Available at: https://готовкцифре.рф (accessed 13.01.2023).

Для цитирования:

Бочарникова М.Е., Пестунова Т.М., Селифанов В.В. Вопросы личной информационной безопасности в условиях цифровой трансформации экономики, управления и общественных коммуникаций // Безопасность цифровых технологий. – 2023. – № 1 (108). – С. 36–52. – DOI: 10.17212/2782-2230-2023-1-36-52.

For citation:

Bocharnikova M.E., Pestunova T.M., Selifanov V.V. Voprosy lichnoi informatsionnoi bezopasnosti v usloviyakh tsifrovoi transformatsii ekonomiki, upravleniya i obshchestvennykh kommunikatsii [Personal information security issues in the context of digital transformation of the economy, management and public communications]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2023, no. 1 (108), pp. 36–52. DOI: 10.17212/2782-2230-2023-1-36-52.