ИНФОРМАЦИОННОЕ ОБЩЕСТВО

DOI: 10.17805/zpu.2022.2.17

Парадокс информационной безопасности в цифровую эпоху

О. В. Гребняк

Институт социально-политических исследований ФНИСЦ РАН

Представленная статья посвящена рассмотрению параллельного развития в современном обществе активной цифровизации двух разнонаправленных тенденций. С одной стороны, речь идет о постепенно растущих и принимающих самые разнообразные формы киберугрозах, реализующихся как через атаки на крупные сайты с целью получения баз данных или остановки производственных процессов, так и через локальное мошенничество в отношении частных лиц: взломы личных страниц, хищение личных данных и денежных средств. С другой стороны, наряду с инцидентами, использующими возможности информационно-коммуникационных технологий, парадоксальным образом в последние годы отмечается снижение числа организаций и граждан, пользующихся возможностями для защиты информации, попадающей в Интернет.

Сами риски компрометации личных данных являются неотъемлемой частью информационно-технологической реальности, оборотной стороной возможности открытого доступа к сетевым коммуникациям и большим объемам информации. Их уровень возможно снизить благодаря навыкам цифровой гигиены. К причинам же пренебрежения средствами информационной защиты можно отнести завышенные ожидания граждан в отношении аппаратной и программной безопасности на фоне заявлений об интенсивном развитии средств защиты и росте выплат на наращивание безопасности, а также чрезмерную самоуверенность на фоне растущих по стране средних показателей цифровой грамотности.

Ключевые слова: информационная безопасность; киберугрозы; цифровая грамотность; цифровизация; безопасность личных данных

ВВЕДЕНИЕ

Информатизация общества и последовавшие за ней процессы цифровой трансформации во всех сферах ведут ко все большему сближению физического мира и цифрового пространства. Именно это стирание граней характеризует четвертую промышленную революцию. Обладая широчайшим экономическим потенциалом и перспективами повышения качества жизни, четвертая промышленная революция, по К. Швабу (Шваб, 2016), несет в себе значимые риски повышения нестабильности. Не в последнюю очередь она окажет влияние на природу общественной и национальной безопасности. Один из аспектов безопасности и будет рассмотрен в рамках статьи.

В России развитие трансформации в последние годы обусловлено направлениями национальной программы «Цифровая экономика Российской Федерации» (в частности, созданием возможности получения госуслуг через удаленный доступ), резким ростом объема интернет-торговли в период пандемии COVID-19 и продолжающей нарастать популярностью социальных сетей. Все перечисленные направления подразумевают размещение большого объема персональных данных, как правило, сопровождаемое разрешением на хранение и обработку личной информации. Тем не менее обеспечить полную сохранность полученных сведений на сегодняшний день невозможно, что подтверждается многочисленными случаями утечки персональных данных и внутренних корпоративных сведений. Несмотря на это, пользователи продолжают свободно размещать личные адреса, номера мобильных телефонов, пересылать рабочую документацию без использования корпоративной почты и позволять сохранять cookies[1] даже при однократном посещении случайных сайтов и т. д.

Так, количество уникальных киберинцидентов в 2020 г. выросло на 51% по сравнению с 2019 г. (Актуальные киберугрозы ... , 2022: Электронный ресурс). В 2021 г. рост продолжился, хотя и значительно замедлился, что подтверждается данными статистики МВД РФ (Краткая характеристика ... , 2022: Электронный ресурс). Уже в первые месяцы 2022 г., по данным «Лаборатории Касперского», число кибератак на российские компании выросло в четыре раза по сравнению с аналогичным периодом 2021 г. (Кильдюшкин, 2022: Электронный ресурс), а геополитическая обстановка позволяет предполагать дальнейшее наращивание их объемов.

В то же время «доля организаций, использовавших средства защиты информации, передаваемой по глобальным сетям», постепенно растущая на участке 2012–2019 гг., внезапно падает в 2020 г. до 75,3% (указанный показатель за 2021 г. на момент подготовки статьи отсутствует). Такую тенденцию демонстрируют данные Мониторинга развития информационного общества, проводимого Росстатом (Мониторинг ... , 2022: Электронный ресурс). Аналогичная «доля населения, использующего средства защиты информации, в общей численности населения, использующего сеть Интернет», начала путь вниз еще раньше — с 2019 г. В период с 2013 по 2018 г. доля населения, использующего средства защиты информации (среди общего числа населения, использующего Интернет) варьировалась между 83,4 и 85,8%. Уже в 2019 г. показатель снизился до 78,5%, продолжив падение в последующие годы. По итогам 2021 г. он составил 72,8%. Таким образом, с 2018 по 2021 г. значение населения, защищающего попадающую в глобальную сеть информацию, упало на 10,6 п.п. (см. табл., с. 240).

Иными словами, уровень развития информационно-коммуникационных технологий (ИКТ), связанных с ними рисков и отношение к соответствующей безопасности на сегодняшний день не вполне коррелируют между собой. Что вызывает опасения, учитывая объемы попадающих в глобальное инфопространство личных сведений, нарастание информационного противостояния и киберугроз. Успешные атаки, создающие помехи производственным и логистическим процессам, финансовым операциям, хищение личных данных и пр. могут стать важными факторами ведущейся информационной войны.

Актуальность затронутого вопроса напрямую связана с обостряющейся геополитической обстановкой, на фоне которой уже сейчас отмечается резкий рост числа внешних атак в цифровой среде. «Фактически ежедневно мощным ударам с при-

ДОЛЯ ОРГАНИЗАЦИЙ И ПОЛЬЗОВАТЕЛЕЙ, ИСПОЛЬЗУЮЩИХ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ, ПОПАДАЮЩЕЙ В ГЛОБАЛЬНУЮ СЕТЬ (2012–2021 гг., %)
SHARE OF ORGANIZATIONS AND USERS THAT USE TOOLS TO PROTECT INFORMATION THAT ENTERS THE GLOBAL NETWORK (2012–2021, PER CENT)

Показатель	*2012*	*2013*	*2014*	*2015*	*2016*	*2017*	*2018*	*2019*	*2020*	*2021*
Доля организаций, использовавших средства защиты информации, передаваемой по глобальным сетям, в общем числе обследованных организаций	85,8	86,7	87,7	86,6	87,3	87,2	89,3	89,5	75,3	—
Доля населения, использующего средства защиты информации, в общей численности населения, использующего сеть Интернет	—	84,7	83,8	85,8	85,3	83,4	83,4	78,5	75,7	72,8

Источник: (Мониторинг ... , 2022: Электронный ресурс)

менением продвинутых информационно-коммуникационных технологий подвергаются государственные учреждения, средства массовой информации, объекты критической инфраструктуры, системы жизнеобеспечения», — заявляет МИД РФ (Заявление МИД России ... , 2022: Электронный ресурс).

Обусловлено ли парадоксальное отношение к вопросам безопасности следствием недостатка информирования об угрозах, низким уровнем цифровой грамотности граждан или иными факторами — ответ на эти вопросы способен построить фундамент для выстраивания стратегии действий по повышению личной ответственности к вопросам цифровой гигиены[2] и, как следствие, к повышению общего уровня информационной безопасности.

Работа проведена на основе анализа открытых эмпирических данных, государственной статистики, отчетов российских экспертов в сфере информационной безопасности.

ДИАЛЕКТИКА ИНФОРМАЦИОННОЙ ДОСТУПНОСТИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Проблема безопасности фундаментальна для социальных наук, как связанная с основными представлениями о человеке и обществе. По мере цивилизационного развития потребность в безопасности постепенно вырастала из границ базовой физической защиты от прямого насилия. Рост частных видов безопасности привел к множественным примерам их систематизации и классификации (Положихина, 2020: 15–16). В перечни попали и виды безопасности, связанные с распространением новых информационно-коммуникационных технологий и процессом цифровизации. Помимо техногенных и производственных вариантов, актуальность набирает безопасность личностная. Чувство защищенности остается одной из базовых

потребностей человека, без которой невозможно стабильное, устойчивое общество (Немировский, Немировская, 2012). Потеря контроля над приватной сферой уничтожает ощущение социальной защищенности.

Информация же начиная с перехода от индустриальных к постиндустриальным общественным отношениям становится основным предметом общественного богатства. Тотальная информатизация, переход в глобальную сеть сначала манили мнимым обещанием ликвидации неравенства по уровню доступности информации и знаний. Но, как показала практика, произошло скорее видоизменение форматов неравенств: например, по технической доступности Интернета, по уровню образования, необходимому и достаточному для восприятия и анализа ставших доступными объемов информации (Donohue, Tichenor, Olien, 1975). С одной стороны, вследствие открытости информации как основного ресурса информационного общества усиливается социальное равенство, с другой — вследствие затрудненности доступа к знанию формируется феномен цифрового неравенства (Костина, 2018).

Сколь бы привлекательны ни были фантазии о прекрасном светлом будущем, но практика подтверждает наивность иллюзий о тождественности глобальной цифровизации и устойчивого мирного развития (Левашов, 2018). Наоборот, транспарентность сетевого пространства, возможность фиксировать цифровой отпечаток личности, так называемый цифровой след, подразумевает постоянную потенциальную угрозу утечек информации и взломов баз данных. «Риски сетевых технологий являются оборотной стороной их перспектив и порождаемых ими социокультурных паттернов» (Аршинов, Асеева, Буданов, и др., 2017: 153–154). И если монетизация личных похищенных данных — скорее порождение новейшего времени, то принципы внедрения информационного противоборства в политической сфере излагал Н. Макиавелли еще в XVI в. (Макиавелли, 2017).

ВНЕШНИЕ КИБЕРАТАКИ И ВНУТРЕННИЕ УТЕЧКИ ИНФОРМАЦИИ

Одна из проблем цифровой трансформации в том, что механизмы обеспечения безопасности не успевают за темпами развития технологий. Тенденция эта характерна не только для России. И в мировой практике не всегда высокий уровень кибербезопасности встречается в странах с сильной информационно-коммуникационной инфраструктурой. «Например, в некоторых странах, у которых хорошо развита ИКТ-инфраструктура, отсутствуют организационные меры для решения проблем кибербезопасности — это Исландия, Швейцария, Дания» (Цифровизация и кибербезопасность … , 2021).

Но значимость обеспечения устойчивости цифровых платформ к внешним и внутренним атакам значимо повышается одновременно с дальнейшим уровнем развития цифровизации. Примером может послужить развитие интернета вещей (Internet of Things, IoT), резко увеличившим вероятность возникновения бреши в безопасности. Персональные данные становятся удобным объектом монетизации в цифровую эпоху. С 2018 г. именно хищение данных является основным мотивом преступников в атаках. В 2021 г. две трети атак на организации были совершены именно с этой целью. Злоумышленники атаковали в том числе и производителей решений для хранения данных. Этот тренд, по ожиданиям экспертов в сфере кибербезопасности, сохранится и в 2022 г.

Каждая третья утечка данных в 2021 г. произошла из высокотехнологичных компаний и сервисов. Доля утечек по вине внутреннего нарушителя (сотрудника самой компании, чьи действия привели к утечке; это может быть как незлонамеренное пренебрежение техникой информационной безопасности, так и умышленный саботаж) в России снизилась с 91% в 2018 г. до 75% в 2021 г. Правда, несколько изменилась их структура: в период с 2019 по 2021 г. взлетела доля утечек умышленного характера (с 58 до 83%). И тем не менее, согласно аналитике InfoWatch, внутренние нарушители все еще остаются главной угрозой информационных активов бизнеса и государственных структур (Россия. Утечки информации … , 2022).

При атаке на компании злоумышленники, как правило, охотятся за учетными и персональными данными сотрудников и информацией, составляющей коммерческую тайну. Доля атак на частных лиц составляет 14% от числа всех атак за год. По статистике разработчика систем информационной безопасности Positive Technologies, за 2021 г. почти половину (46%) украденной информации составили учетные данные. Пятая часть от общего объема украденной информации — персональные сведения. Частные компьютеры и сетевое оборудование стали объектами атак в 37% случаев, а каждая четвертая атака была нацелена на мобильные устройства. В результате успешных атак в большинстве случаев устройства заражались ПО для удаленного управления, шпионским ПО и банковскими «троянами». Источником заражения чаще всего становились электронная почта (30%) и сайты (33%) (Актуальные киберугрозы … , 2022: Электронный ресурс).

Стоит обратить внимание, что везде речь идет о получении персональных данных. Если в случае государственных и медицинских учреждений у граждан преимущественно нет выбора, они обязаны предоставить определенный объем сведений, то во многих случаях сбор дополнительной информации о месте проживания, номере телефона, сохранение данных банковской карты для «быстрых платежей» осуществляется при попустительстве самих граждан.

ЦИФРОВАЯ ГРАМОТНОСТЬ ГРАЖДАН И УКРЕПЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Можно ли оправдать парадоксальное отношение организаций и граждан к безопасности информации отсутствием цифровой грамотности и сокрытием компаниями сведений об объемах утечек данных?

Все перечисленные выше отчеты разработчиков систем безопасности, статистика, данные Министерства внутренних дел находятся в открытом доступе. Инциденты успешных атак и факты появления в открытом доступе похищенных баз данных периодически освещаются новостными агентствами.

За последние годы финансирование разработок и внедрения систем безопасности различных уровней в сфере ИКТ только растет. Федеральным бюджетом на исполнение проекта «Информационная безопасность» (нацпроект «Цифровая экономика Российской Фежерации») в 2021 г. было выделено 3 млрд руб. На 2022 г., согласно отчету Казначейства на 1 марта 2022 г., утверждена сумма в размере почти 8,5 млрд руб. (Федеральный бюджет … , 2022: Электронный ресурс). Снижение в данных условиях доли организаций, использующих средства защиты передаваемой в глобальную сеть информации (напомню, с достигнутого в 2019 г. значимого уровня в 89,5% доля таких организаций упала в 2020 г. до 75,3%), по меньшей мере нелогично.

Ситуация с общим уровнем цифровой грамотности среди населения страны в целом развивается неплохо. Общий индекс цифровой грамотности россиян по данным на май 2022 г. составил 64 пункта (из 100 возможных), демонстрируя положительную тенденцию — годом ранее индекс составлял 58 пунктов) (Уровень цифровой грамотности ... , 2022: Электронный ресурс; Вынужденная цифровизация ... , 2021: Электронный ресурс).

Если углубиться в эти показатели, картина значительно изменится. Внутри общего индекса продолжает сокращаться доля граждан с начальным уровнем цифровой грамотности (2020 г. — 7%, 2021 г. — 4%, 2022 г. — 3%). На прежнем уровне за год осталось число россиян, обладающих базовыми компетенциями (2020 г. — 66%, 2021 г. — 70%, 2022 г. — 70%). При этом очередной год в стагнации находится доля граждан с продвинутым уровнем цифровых компетенций: весь рассмотренный период она сохраняется на уровне 27%, что ниже заложенных паспортом федерального проекта «Кадры для цифровой экономики». Упомянутый документ задает следующий уровень целевых значений по доле россиян, обладающих цифровой грамотностью и ключевыми компетенциями цифровой экономики: 27% на 2019 г.; 30% на 2020 г.; 32% на 2021 г.; 36% на 2022 г. и далее по нарастающей (Паспорт федерального проекта ... : Электронный ресурс).

Еще большее понимание поведения пользователей сети дают результаты опроса, исследующего отношение россиян к защите персональных данных, проведенного в середине 2021 г. При том что 63% россиян не считают защищенными свои персональные данные в Интернете, тем не менее резко растет число респондентов, желающих снять с себя ответственность за безопасность. Доля граждан, которые считают, что следить за сохранностью информации должны в первую очередь владельцы сайтов, провайдеры сервисов или государство, в 2021 г. достигло 81% (62% в 2018 г.; 61% в 2020 г.) (Отношение россиян ... : Электронный ресурс).

В целом автор согласен с тем, что максимальная безопасность хранения персональной информации (паспортные данные, медицинские сведения, номера телефонов и данных о банковских счетах и пр.) должна предоставляться по умолчанию в случае, когда ее предоставление необходимо (Левашов, Гребняк, 2020). Но объемы скомпрометированных за последние годы данных говорят о явной преждевременности пренебрежения цифровой гигиеной в ближайшие годы.

ЗАКЛЮЧЕНИЕ

Рост государственного финансирования на разработку и внедрение аппаратной и программной защиты в информационной среде и распространяемые общие данные по среднему росту цифровой грамотности приводят к более расслабленному отношению граждан. Пользуясь сетевыми услугами и цифровыми технологиями, они переносят с себя ответственность на якобы высокозащищенные сервера, облачные хранилища и программное обеспечение, игнорируя требования цифровой гигиены. Это и приводит рано или поздно к срабатыванию «человеческого фактора», занимающего не последнее место в инцидентах с безопасностью. 80% компаний считают, что внутренние инциденты опаснее, чем угрозы извне (Исследование уровня информационной безопасности ... : Электронный ресурс).

Общая положительная статистика цифровой грамотности среди россиян, истории успешного противодействия телефонным и интернет-мошенникам, обсуждение в сети популярных методик отдельных злоумышленников укрепляют ложную

уверенность «я умнее, со мной такое не пройдет». Высокая мотивация приводит к постоянному появлению у мошенников все новых схем, а самоуверенность граждан — к их успешной реализации.

Рассмотренный феномен полностью вписывается в общий образ парадоксальных сочетаний, характерных для развития информационного общества. Например, речь о сочетаниях «информация — ложная информация»; «обширные объемы доступной информации — отсутствие когнитивных возможностей для ее полного усвоения» (Тузовский, 2015: 27–29; Павликова, 2008: 85–87) и многих других. В отличие от описанного в статье примера, они являются неотъемлемыми категориями информационного общества. В то время как парадоксальное отношение к информационной безопасности в периоды постоянно растущей угрозы есть вероятность преобразовать в ходе дальнейшей работы проектов по подготовке кадров для цифровой экономики. К примеру, за счет контроля и проверки практического применения защитных мер, так как практика показывает, что теоретическое информирование об опасностях результата не приносит. Альтернативой может стать разработка практической программы отработки соответствующих навыков в коллаборации с профильными психологами, так как мотивация и выбор успешного формата наработки навыков может во многом зависеть от базового уровня подготовки, индивидуальных характеристик сотрудников и даже сферы деятельности той или иной организации.

ПРИМЕЧАНИЯ

[1] Cookies (англ.: печеньки) — фрагмент данных о посещении определенного веб-сервера, хранимый на компьютере пользователя. При повторном выходе на соответствующий сайт браузер пересылает этот фрагмент данных на сервер. Используется для сохранения логина-пароля, хранения персональных настроек, сбора различных сведений о пользователях (объем собираемой информации зависит от настроек). Cookie возможно перехватить (например, для доступа к чужой учетной записи), если пользователь применяет нешифрованное соединение с сервером, в частности при использовании публичных точек доступа Wi-Fi.

[2] «Цифровая гигиена» — базовые приемы, обеспечивающие личную информационную безопасность (не путать с анонимностью) в Интернете. Касаются стандартных вопросов создания и регулярного обновления сложных паролей; хранения сканов важных документов вне облачных хранилищ; формулировки действительно секретных вопросов вместо достаточно открытой информации о девичьей фамилии матери или кличке питомца; отказ от перехода по ссылкам от незнакомых адресантов и прочее. Термин предположительно впервые прозвучал в статьях журналиста Н. С. Митрохина в газете «Московская правда» в 2013 г.

СПИСОК ЛИТЕРАТУРЫ

Актуальные киберугрозы: итоги 2021 года [Электронный ресурс] // Positive Technologies. URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cyberse-curity-threatscape-2021-rus.pdf (дата обращения: 16.04.2022).

Аршинов, В. И., Асеева, И. А., Буданов, В. Г. [и др.] (2017) Социо-антропологические измерения конвергентных технологий. Модели, прогнозы, риски. Курск : Университетская книга, 2017. 243 с.

Вынужденная цифровизация: исследование цифровой грамотности россиян в 2021 году [Электронный ресурс] // Аналитический центр НАФИ. URL: https://nafi.ru/analytics/vynuzhdennaya-tsifrovizatsiya-issledovanie-tsifrovoy-gramotnosti-rossiyan-v-2021-godu/ (дата обращения 16.04.2022).

Заявление МИД России в связи с продолжающейся киберагрессией со стороны «коллективного Запада» [Электронный ресурс] // МИД РФ. URL: https://www.mid.ru/ru/foreign_policy/news/1806906/ (дата обращения: 04.04.2022).

Исследование уровня информационной безопасности в компаниях России и СНГ за 2020 год [Электронный ресурс] // SearchInform. URL: https://searchinform.ru/survey/global-2020 (дата обращения: 16.04.2022).

Кильдюшкин, Р. (2022) В «Лаборатории Касперского» сообщили о росте кибератак на российские компании [Электронный ресурс] // Газета.Ру. URL: https://www.gazeta.ru/tech/news/2022/03/25/17472103.shtml (дата обращения: 16.04.2022).

Костина, А. В. (2018) Информатизация и тенденции развития общества XXI века // Знание. Понимание. Умение. №1. С. 143–156. DOI 10.17805/zpu.2018.1.11

Краткая характеристика состояния преступности в РФ за январь — декабрь 2021 года [Электронный ресурс] // Официальный сайт МВД РФ. URL: https://мвд.рф/reports/item/28021552/ (дата обращения: 16.04.2022).

Левашов, В. К. (2018) Трансформации информационной сферы гражданского общества // Наука. Культура. Общество. №2–3. С. 112–123.

Левашов, В. К., Гребняк, О. В. (2020) Есть ли место личным данным в цифровом будущем? // Вестник РГГУ. Серия Философия. Социология. Искусствоведение. №4. С. 57–71. DOI: 10.28995/2073-6401-2020-4-57-71

Макиавелли, Н. (2017) Государь / пер. с итал. и прим. М. Юсима. СПб. : Азбука. 447 с.

Мониторинг развития информационного общества [Электронный ресурс] // Росстат. URL: https://rosstat.gov.ru/folder/154882 (дата обращения: 16.04.2022).

Немировский, В. Г., Немировская, А. В. (2012) Чувство незащищенности от социальных опасностей как основа типологизации регионов // Мониторинг общественного мнения. №1 (107). С. 113–127.

Отношение россиян к защите персональных данных [Электронный ресурс] // Аналитический центр НАФИ. URL: https://nafi.ru/projects/it-i-telekom/otnoshenie-rossiyan-k-zashchite-personalnykh-dannykh/ (дата обращения: 16.04.2022).

Павликова, М. М. (2008) Парадоксы информационного общества // Вестник Московского университета. Серия 10: Журналистика. №1. С. 82–91.

Паспорт федерального проекта «Кадры для цифровой экономики» [Электронный ресурс] // Цифровая экономика 2024. URL: https://digital.ac.gov.ru/poleznaya-informaciya/material/Паспорт-федерального-проекта-Кадры-для-цифровой-экономики.pdf (дата обращения: 16.04.2022).

Положихина, М. А. (2020) Влияние цифровизации на безопасность: от индивидуума до социума // Социальные новации и социальные науки. №1. С. 9–27. DOI: 10.31249/snsn/ 2020.01.01

Россия. Утечки информации ограниченного доступа в 2021 году: аналитический отчет // Экспертно-аналитический центр InfoWatch. 2022. 27 с.

Тузовский, И. Д. (2015) Парадоксы информационного общества // Информационное общество. №6. С. 25–34.

Уровень цифровой грамотности в России и Беларуси [Электронный ресурс] // Аналитический центр НАФИ. URL: https://nafi.ru/analytics/uroven-tsifrovoy-gramotnosti-v-rossii-i-belarusi/ (дата обращения: 16.04.2022).

Федеральный бюджет в разрезе нацпроектов за 2022 год [Электронный ресурс] // Госрасходы. URL: https://spending.gov.ru/budget/np/?year=2022 (дата обращения: 16.05.2022).

Цифровизация и кибербезопасность: аналитический отчет // Экспертно-аналитический центр InfoWatch. 2021. 33 с.

Шваб, К. (2016) Четвертая промышленная революция. М. : Эксмо. 208 с.

Donohue, G. A., Tichenor, P. J. and Olien C. N. (1975) Mass Media and the Knowledge Gap. A Hypothesis Reconsidered // Communication Research. Vol. 2. №1. P. 3–23. DOI: 10.1177/009365027500200101

Дата поступления: 20.04.2022 г.

PARADOX OF INFORMATION SECURITY IN THE DIGITAL AGE

O. V. GREBNYAK
FCTAS RAS INSTITUTE OF SOCIO-POLITICAL RESEARCH

This article examines the parallel development of two multidirectional trends in the modern society of active digitalization. On the one hand, we are talking about gradually growing and taking a variety of forms cyber threats, executed both through attacks on large sites in order to obtain databases or stop production processes, and through local fraud against individuals: breaking into personal pages, stealing personal data and money. On the other hand, along with incidents that exploit the capabilities of information and communication technologies, there has been a paradoxical decrease in the number of organizations and citizens making use of opportunities to protect information that enters the Internet in recent years.

The very risks of compromising personal data are part and parcel of the information technology reality, the flip side of the possibility of open access to network communications and large volumes of information. It is possible to reduce their level by practicing digital hygiene. The reasons for the neglect of information security include the overestimated expectations of citizens regarding hardware and software security against the background of statements about the intensive development of security tools and the growth of payments to build security, as well as excessive self-confidence against the growing national average rates of digital literacy.

Keywords: information security; cyber threats; digital literacy; digitalization; personal data security

REFERENCES

Aktual'nye kiberugrozy: itogi 2021 goda. *Positive Technologies* [online] URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2021-rus.pdf (accessed: 16.04.2022). (In Russ.).

Arshinov, V. I., Aseeva, I. A., Budanov V. G. et al. (2017) *Sotsio-antropologicheskie izmereniia konvergentnykh tekhnologii. Modeli, prognozy, riski* [online] Kursk, Universitetskaia kniga. 243 p. (In Russ.).

Vynuzhdennaia tsifrovizatsiia: issledovanie tsifrovoi gramotnosti rossiian v 2021 godu. *Analiticheskii tsentr NAFI* [online] URL: https://nafi.ru/analytics/vynuzhdennaya-tsifrovizatsiya-issledovanie-tsifrovoy-gramotnosti-rossiyan-v-2021-godu/ (accessed: 16.04.2022). (In Russ.).

Zaiavlenie MID Rossii v sviazi s prodolzhaiushcheisia kiberagressiei so storony «kollektivnogo Zapada». *MID RF* [online] URL: https://www.mid.ru/ru/foreign_policy/news/1806906/ (accessed: 04.04.2022). (In Russ.).

Issledovanie urovnia informatsionnoi bezopasnosti v kompaniiakh Rossii i SNG za 2020 god. *SearchInform* [online] URL: https://searchinform.ru/survey/global-2020 (accessed: 16.04.2022). (In Russ.).

Kil'diushkin, R. (2022) V «Laboratorii Kasperskogo» soobshchili o roste kiberatak na rossiiskie kompanii. *Gazeta.Ru* [online] URL: https://www.gazeta.ru/tech/news/2022/03/25/17472103.shtml (accessed: 16.04.2022). (In Russ.).

Kostina, A. V. (2018) Informatizatsiia i tendentsii razvitiia obshchestva XXI veka. *Znanie. Ponimanie. Umenie*, no. 1, pp. 143–156. DOI 10.17805/zpu.2018.1.11 (In Russ.).

Kratkaia kharakteristika sostoianiia prestupnosti v RF za ianvar'-dekabr' 2021 goda. *Ofitsial'nyi sait MVD RF* [online] URL: https://mvd.rf/reports/item/28021552/ (accessed: 16.04.2022). (In Russ.).

Levashov, V. K. (2018) Transformatsii informatsionnoi sfery grazhdanskogo obshchestva. *Nauka. Kul'tura. Obshchestvo*, no 2–3, pp. 112–123. (In Russ.).

Levashov, V. K. and Grebniak, O. V. (2020) Est' li mesto lichnym dannym v tsifrovom budushchem? *Vestnik RGGU. Seriia «Filosofiia. Sotsiologiia. Iskusstvovedenie»*, no. 4, pp. 57–71. DOI: 10.28995/2073-6401-2020-4-57-71 (In Russ.).

Makiavelli, N. (2017) *Gosudar'* / transl. from Italian and notes by M. Iusima. St. Petersburg, Azbuka. 447 p. (In Russ.).

Monitoring razvitiia informatsionnogo obshchestva. *Rosstat* [online] URL: https://rosstat.gov.ru/folder/154882 (accessed: 16.04.2022). (In Russ.).

Nemirovskii, V. G. and Nemirovskaia, A. V. (2012) Chuvstvo nezashchishchennosti ot sotsial'nykh opasnostei kak osnova tipologizatsii regionov. *Monitoring obshchestvennogo mneniia*, no. 1 (107), pp. 113–127. (In Russ.).

Otnoshenie rossiian k zashchite personal'nykh dannykh. *Analiticheskii tsentr NAFI* [online] URL: https://nafi.ru/projects/it-i-telekom/otnoshenie-rossiyan-k-zashchite-personalnykh-dannykh/ (accessed: 16.04.2022). (In Russ.).

Pavlikova, M. M. (2008) Paradoksy informatsionnogo obshchestva. *Vestnik Moskovskogo universiteta. Seriia 10: Zhurnalistika*, no. 1, pp. 82–91. (In Russ.).

Pasport federal'nogo proekta «Kadry dlia tsifrovoi ekonomiki». *Tsifrovaia ekonomika 2024* [online] URL: https://digital.ac.gov.ru/poleznaya-informaciya/material/Pasport-federal'nogo-proekta-Kadry-dlia-tsifrovoi-ekonomiki.pdf (accessed: 16.04.2022). (In Russ.).

Polozhikhina, M. A. (2020) Vliianie tsifrovizatsii na bezopasnost': ot individuuma do sotsiuma. *Sotsial'nye novatsii i sotsial'nye nauki*, no. 1, pp. 9–27. DOI: 10.31249/snsn/2020.01.01 (In Russ.).

Rossiia. Utechki informatsii ogranichennogo dostupa v 2021 godu: analiticheskii otchet. *Ekspertno-analiticheskii tsentr InfoWatch*. 2022. 27 p. (In Russ.).

Tuzovskii, I. D. (2015) Paradoksy informatsionnogo obshchestva. *Informatsionnoe obshchestvo*, no. 6, pp. 25–34. (In Russ.).

Uroven' tsifrovoi gramotnosti v Rossii i Belarusi. *Analiticheskii tsentr NAFI* [online] URL: https://nafi.ru/analytics/uroven-tsifrovoy-gramotnosti-v-rossii-i-belarusi/ (accessed: 16.04.2022). (In Russ.).

Federal'nyi biudzhet v razreze natsproektov za 2022 god. *Gosraskhody* [online] URL: https://spending.gov.ru/budget/np/?year=2022 (accessed: 16.04.2022). (In Russ.).

Tsifrovizatsiia i kiberbezopasnost': analiticheskii otchet. *Ekspertno-analiticheskii tsentr InfoWatch*. 2021. 33 p. (In Russ.).

Shvab, K. (2016) Chetvertaia promyshlennaia revoliutsiia. Moscow, Eksmo. 208 p. (In Russ.).

Donohue, G. A., Tichenor, P. J. and Olien C. N. (1975) Mass Media and the Knowledge Gap. A Hypothesis Reconsidered. *Communication Research*, vol. 2, no 1, pp. 3–23. DOI: 10.1177/009365027500200101

Submission date: 20.04.2022.

Гребняк Оксана Валерьевна — младший научный сотрудник Центра социальных и социально-политических исследований, ИСПИ ФНИСЦ РАН. Адрес: 119333, Россия, г. Москва, ул. Фотиевой, д. 6, стр. 1. Тел.: +7 (499) 530-27-32. Эл. адрес: oksananov@yandex.ru

Grebnyak Oksana Valeryevna, Junior Researcher, Center for Social and Socio-Political Research, ISPR FCTAS RAS. Postal address: 6, Fotievoi St., Bldg. 1, Moscow, Russian Federation, 119333. Tel.: +7 (499) 530-27-32. E-mail: oksananov@yandex.ru