НАУЧНАЯ СТАТЬЯ
JEL: M15, M21
УДК: 65.011.56

ДОСТОВЕРНОСТЬ ИНФОРМАЦИИ В ЦИФРОВОМ ОБОРОТЕ ДАННЫХ

Татьяна Алексеевна Рудакова
кандидат экономических наук, доцент кафедры экономики и финансов Алтайского государственного технического университета им. И. И. Ползунова, кафедры экономической безопасности, учета, анализа и аудита Алтайского государственного университета, Россия, Барнаул, aleks_rudakova@mail.ru, ORCID: 0000–0002–8735–7058

Резюме. Активный переход данных в цифровое пространство способствует тому, что качество и достоверность информации приобретает особую значимость, определяя точность управленческих решений и надежность информационного обмена. Автором проведен анализ причинно-следственных связей наличия и обращения в интернет-пространстве информации, не соответствующих обеспечению ее базовой характеристике — достоверности. Результатом исследования стал расширенный перечень проблем и способов обеспечения защиты и достоверности информации через воспитание и повышение уровня развития навыков цифровой гигиены поставщиков и пользователей информационного продукта; увеличение количества бизнес-структур, прибегающих к услугам IT-компаний за приобретением продуктов, снижающих вероятность информационной незащищенности; ускорение темпов развития защитных функций ИТ-решений в цифровом обмене данными; формирование концепции применения методов социальной инженерии для защиты участников цифрового поля.

Ключевые слова: достоверность информации, оборот данных, цифровая экономика, информационная безопасность, оценка риска

Для цитирования: Рудакова Т. А. Достоверность информации в цифровом обороте данных // Управление современной организацией: опыт, проблемы и перспективы. 2025. № 23. С. 20–28.

RELIABILITY OF INFORMATION IN DIGITAL DATA CIRCUIT

Tatyana A. Rudakova
Candidate of Economic Sciences, Associate Professor, Department of Economics and Finance, I. I. Polzunov Altai State Technical University, Department of Economic Security, Accounting, Analysis and Audit, Altai State University, Barnaul, Russia, aleks_rudakova@mail.ru ORCID: 0000–0002–8735–7058

Resume. The active transition of data to the digital space contributes to the fact that the quality and reliability of information is of particular importance, determining the accuracy of management decisions and the reliability of information exchange. The author analyzed the cause-and-effect relationships of the presence and circulation of information in the Internet space that do not correspond to ensuring its basic characteristic — reliability. The result of the study was an expanded list of problems and ways to ensure the protection and reliability of information through education and raising the level of development of digital hygiene skills of suppliers and users of the information product; an increase in the number of business structures resorting to the services of IT companies for the purchase of products that reduce the likelihood of information insecurity; accelerating the pace of development of protective functions of IT solutions in digital data exchange; the formation of a concept for the use of social engineering methods to protect participants in the digital field.

Keywords: reliability of information, data circulation, digital economy, information security, risk assessment

For citation: Rudakova T. A. Reliability of Information in Digital Data Circuit. *Upravlenie sovremennoj organizaciej: opyt, problemy i perspektivy = Management of the Modern Organization: Experience, Problems and Perspectives*. 2025;23:20–28. (In Russ.).

Информация как феномен или продукт цифрового мира

Научная литература определяет данные как сведения, факты и показатели. Форма представления данных может быть любой, в том числе и в виде чисел. Преобразование, обобщение и передача данных превращает (преобразует) их в информацию различного характера. Термин «информация» образован от латинского *informatio*, что означает изложение, разъяснение какого-либо факта, события, явления. В философском словаре М. Розенталя информация (лат. *Informatio* — разъяснение, изложение) — некоторые сведения, совокупность каких-либо данных.

Феномен «информация» интересовал пытливые умы на протяжении длительного периода времени, что выразилось в значительном количестве подходов к определению значений данного термина и формулировании теорий различного характера — статической, прагматической. Значительный спектр теорий посвящен исследованию разнообразных сторон термина «информация». Не вступая в противоречия, являясь дополнением друг друга, они не опровергают, а отображают особенности ее отдельных сторон. «При этом всегда имеется в виду задача — если не полного, то частичного — синтеза этих теорий» (Дубровский, 1996). Однако, по мнению К. Шеннона, необходимо учитывать, что базовые положения теорий всегда посвящены специфическим направлениям исследования феномена информации, а это не предполагает положительного результата в других социальных науках, таких как, например, психология или экономика (Шеннон, 1963).

Согласно утверждению Г. Штейнбуха понятие «информация» наряду с терминами «материя» и «энергия» не имеет исчерпывающего и полного определения (Городов, 2021).

Информация отличается индивидуальными характеристиками, к которым следует отнести содержание, объем, форму представления, источник и способ передачи и, конечно, потребителя.

Вытеснение аналоговых технологий технологиями нового поколения для генерирования и передачи данных привело к появлению термина «цифровая информация», которая рассматривается как разновидность информации электронного вида. Особенностью информации такого вида является способ ее фиксации, хранения и передачи посредством информационно-телекоммуникационных технологий.

Закон «Об информации, информационных технологиях и о защите информации» определяет ряд понятий, связанных с оборотом данных (рис. 1). В условиях цифровой трансформации социально-экономических процессов, информационного общества, или общества знаний, возникает желание расширить данный список, включив словосочетания: цифровая грамотность, цифровая зрелость, цифровая трансформация, цифровая гигиена, цифровая платформа.

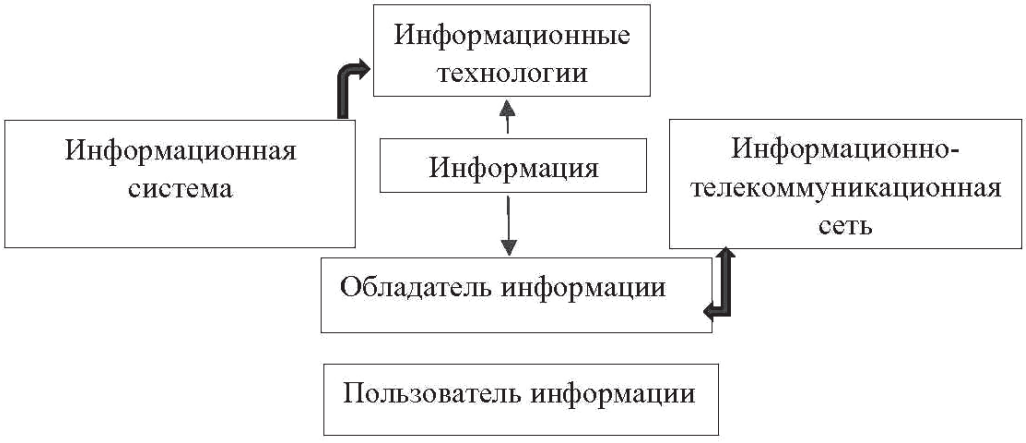

Рисунок 1 — Объекты и субъекты информационного пространства[1]
Figure 1 — Objects and subjects of information space

[1] Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 №149-ФЗ (с послед. изм. и доп.).

Цифровой мир открыл новые возможности в организации бизнес-процессов — размещение структурных подразделений на различных территориях, перевод рабочих мест в виртуальное пространство, коммуникация персонала посредством электронного документооборота, использование облачных сервисов. Система образования активно внедряет в образовательный процесс форму дистанционного обучения, используя для этих целей электронные платформы и размещая на них образовательный контент. Генеративный искусственный интеллект проникает в различные сферы деятельности, отрасли, государственное управление, выполняя отдельные функции, которые еще не так давно были исключительно прерогативой человека.

Использование современных решений ИТ-отрасли обеспечивает развитие хозяйствующих субъектов и социально-экономических отношений.

По предварительной оценке специалистов информационного источника TADVISER, объем российского рынка ИТ-услуг в 2024 г. может составить порядка 717 млрд руб.[2]

Таблица 1

Объем российского рынка ИТ-услуг в оценке TADVISER, млрд руб.

Table 1

Volume of the Russian IT services market as assessed by TADVISER, billion rubles

2019 г.	2020 г.	2021 г.	2022 г.	2023 г.	2024 г. (предв. оценка)
373,4	422	485,3	582	652	717

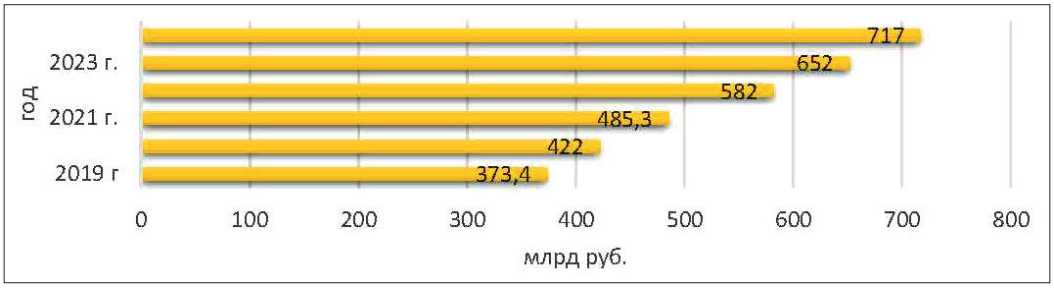

Рисунок 2 — Объем российского рынка ИТ-услуг в оценке TADVISER, млрд руб.
Figure 2 — Volume of the Russian IT services market as assessed by TADVISER, billion rubles

Достоверность информации цифрового пространства

Достоверность информации приобретает большую актуальность, поскольку растущие возможности передачи информации способствуют желанию либо изменить ее содержание, либо стать обладателем в единственном лице, либо передать не по назначению. Положительное влияние цифровой трансформации на процессы, происходящие в обществе, не исключает отрицательных моментов в получении и использовании результатов происходящих преобразований. Цифровые двойники сайтов экономических структур, площадок электронной торговли не только вводят в заблуждение пользователей информации, но и провоцируют финансовые потери. Электронные образовательные технологии не гарантируют формирования компетенций в полном объеме.

Современное общество сталкивается с проблемой достоверности информации в информационных системах, цифровых платформах, сервисах, размещение которой преследует различные цели как экономического, так и политического характера. Пользователи информации, определяя свои стратегические цели, анализируют данные, не отвечающие требованиям цифрового общества, или общества знания, как нового типа общества. «В экономике, основанной на знаниях, под термином „знания" понимается не только массив информации, которым обладают конкретные люди, но и часть продукта или услуги» (Гапоненко, 2008). Преобладающее значение в обществе знания отводится достоверной информации — как источнику развития субъектов взаимоотношений, экономики отдельного хозяйствующего субъекта, территории и государства. В Стратегии развития информационного общества РФ на 2017–2030 гг.[3] достоверность

[2] Российский рынок ИТ-услуг и аутсорсинга // Tadviser. Государство. Бизнес. Технологии. URL: https://goo.su/QEDfN

[3] О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы : Указ Президента РФ от 09.05.2017 №203.

информации рассматривается как один из основных критериев перехода к обществу знания. Информационные процессы и цифровые технологии функционируют как единое целое. Однако предполагаемая идиллия омрачается фактом присутствия в информационном поле массива недостоверных данных. Поставщиком данного продукта могут выступать хозяйствующие субъекты, физические и юридические лица, а на потребителя возлагается необходимость выделения из массива данных информации, которая должна отвечать в первую очередь признакам достоверности и лишь затем быть релевантной. Эффективность оборота цифровых данных в условиях электронного обмена может быть оценена только с корректировкой на достоверность.

В научной литературе достоверность рассматривается сквозь призму соответствия характеристике предмета, о котором повествует. Так, например, достоверной считается информация, формируемая в бухгалтерском учете, при условии соблюдения требований стандартов в процессе сбора, фиксации и обобщения согласно нормативно-правовой базе. Учетная система, построенная на принципах международных стандартов, в отношении информации, размещаемой отчитывающейся компанией, использует термин «правдивость» информации, которая характеризуется точностью исчисления и отсутствием ошибок. Информация, характеризующая имущественное положение, движение денежных средств и результаты финансово-хозяйственной деятельности, — финансовая отчетность формирует государственный информационный ресурс. Такая информация, размещаемая на цифровой платформе государственного значения, заслуживает доверия для пользователей. За достоверное представление информации о предприятии ответственность несет его руководство, кроме того, институт аудита проверяет качество такой информации, выражая профессиональное (экспертное) мнение об отсутствии или наличии существенных искажений. Следует отметить, что не все хозяйствующие субъекты обязаны подтверждать соответствие данных отчетности независимыми экспертами — только юридические лица, имеющие статус публичных компаний или значительную стоимость активов и выручки. Что же касается компаний других организационно-правовых форм, компаний, не отличающихся внушительными масштабами бизнеса, стоимостью активов и полученного дохода, то стоит, видимо, лишь надеяться на соблюдение всех регулятивов.

Риски и источники (средства) преодоления

По мнению ряда специалистов, опасными в настоящий момент остаются не только сообщения индивидуального характера, но и цифровые платформы, сервисы, функционирующие на информации несоответствующего качества. Извлекая дополнительную ренту от такого рода деятельности и вводя в заблуждение пользователей, они увеличивают вероятность риска необоснованных управленческих решений. Как видится, верным и актуальным в современном обществе знания звучит утверждение древнегреческого философа: «гораздо больше риска в приобретении знаний, чем в покупке съестного» (Сократ. Я ничего не знаю, 2024).

Проблема достоверности информации в цифровом обороте данных требует решения в краткосрочной перспективе, поскольку порождает дополнительные сложности, которые требуют большего объема ресурсов для их преодоления.

На этапе подготовки информации отчитывающейся организацией от момента фиксации и до передачи в цифровое пространство она преодолевает ряд «фильтров»: систему внутреннего контроля (для каждой организации), внешнего независимого эксперта в лице аудиторской организации (в обязательном порядке либо добровольно), камеральную проверку при поступлении в базу государственного информационного ресурса бухгалтерской (финансовой) отчетности (ГИР БО). Можно утверждать, что определенный порог качества — достоверности информационного продукта гарантирован пользователям. Фальсификация и преднамеренное искажение данных в большинстве случаев происходит по причине несанкционированного доступа с использованием достижений ИТ-отрасли, утечкой информации через сотрудников как по неосторожности, так и преднамеренно. Что касается информации, раскрывающей персональный характер ее собственника, то причиной утечки является несоблюдение цифровой гигиены в интернет-пространстве и при работе с финансовыми инструментами, а также приемы социальной инженерии лицами, желающими ее получить. Это выливается в различного рода потери — финансового, морального, репутационного характера и возникновение кредитных обязательств (табл. 2).

В достоверности информации, которая стала продуктом генеративного искусственного интеллекта, в настоящее время можно усомниться по причине того, что генерирование определенного вида информации осуществляется с использованием данных, предоставленных интеллектуальной системе человеком и не всегда проверенных и соответствующих действительности. С одной стороны, искусственный интеллект может выступать помощником в процессе выявления манипуляций с информацией и использованием ее в противоправных действиях, ограничивающим возможность поставки недостоверной информации в цифровое пространство, с другой — быть поставщиком такой информации.

Таблица 2

Правонарушения в области информационных технологий

Table 2

Information technology offenses

Виды правонарушений	Риски	Последствия	Защита	Борьба	
				УК РФ	Пользователь
Распространение вредоносных программ	Передача информации неопределенному кругу лиц	Потеря данных	Проверенные сайты. Антивирусные программы. Оригинальные интернет-ссылки	Ст. 273 УК РФ	Удаление с использованием антивирусных программ
Фишинг	Доступ к логину и паролю	Финансовые и репутационные потери, утрата личной информации, моральный ущерб	Оригинальные интернет-ссылки. Хранение личных данных. Антифишинговое ПО	Ст. 272 УК РФ	Изменить логины и пароли затронутых фишингом аккаунтов
Взлом паролей	Доступ к охраняемой законом информации	Потеря значимой информации	Не передавать личные данные третьим лицам. Не размещать личные данные в мессенджерах. Игнорировать подозрительные сообщения на почте. Использовать сложные пароли	Ст. 272 УК РФ	Изменить логины и пароли взломанных аккаунтов
Кража банковских реквизитов	Доступ к денежным средствам	Финансовые потери	Устанавливать приложения из проверенных источников. Блокировка банковской карты при утрате мобильного телефона. Блокировка банковской карты. Игнорировать звонки и сообщения с незнакомых номеров Покупки в проверенных интернет-магазинах. Использование банкоматами в проверенных охраняемых местах	Ст. 15 УК РФ, п. «г», ч. 3 ст. 158 УК РФ	Блокировка банковской карты в мобильном приложении, либо в отделении банка, либо при помощи звонка в банк
Распространение противоправной информации через интернет	Дискредитация	Репутационные потери			
Мошенничество	Доступ к денежным средствам. Ложная информация	Финансовые потери и возникновение финансовых обязательств	Игнорировать сообщения о крупных выигрышах, в случае если вы нигде не участвовали. Поверять товары перед их покупкой в интернете (характеристика товара, цена). Исключить предоплату товара. Исключить покупку билетов на сомнительных сайтах (самолет, поезд, концерт и т. п.)	Ст. 159.6 УК РФ	Обращение в полицию
Вмешательство в работу различных систем	Доступ к данным юридического или физического лица	Потеря данных и использование в мошеннических целях		Ст. 274 УК РФ	Органы по борьбе с киберпреступностью

Составлено по данным[4]

По данным АО «Лаборатория Касперского» в 2024 г. остановлено 437 млн кибератак, заблокировано 106 млн уникальных вредоносных ссылок, нейтрализовано 112 млн уникальных вредоносных объектов[5]. Банк России, в свою очередь, составил

[4] Попов А. Правонарушения в области информационных технологий. URL: https://vc.ru/u/1393633-popov-aleksei/574746-pravonarusheniya-v-oblasti-informacionnyh-tehnologii

[5] Сайт АО «Лаборатория Касперского». URL: https://www.kaspersky.ru/

Рисунок 3 — Портрет пострадавшего от кибермошенничества, %
Figure 3 — Portrait of a victim of cyber fraud, %

портрет пострадавшего физического лица от кибермошенничества (рис. 3)[6].

Результат опроса показал, что наибольший процент пострадавших — это городское население, респонденты от 25 до 44 лет, женщины, со средним образованием и уровнем дохода. Список приемов кибермошенников в 2024 г. пополнился несанкционированным доступом к аккаунту на сайте Госуслуг. Первое место данного списка занимают результаты телефонных звонков или СМС, далее по убыванию — атаки через мессенджеры, социальные сети, сообщения по электронной почте, использование фишинговых ресурсов, поддельные QR-коды.

По данным компании по управлению цифровыми рисками BI.ZONE в 2024 г. около 400 организаций получили фишинговые письма от имени государственных органов со ссылками на вредоносные файлы в виде PDF-документов, уведомляющих о правонарушениях в области налогового законодательства. Осуществить такое мероприятие позволило мошенникам вполне легитимное средство удаленного доступа — NetSupport (программное обеспечение для удаленного управления). Кроме того, как отмечают специалисты компании BI.ZONE Threat Intelligence, от действий компании хакерской группы Bloody Wolf пострадали компании финансового сектора, компании, оказывающие транспортные услуги, услуги логистического характера, представители IT-отрасли. Результаты анализа защищенности в области информационной безопасности, по данным компании «Бастион», свидетельствуют о том, что 65% организаций, получивших в компании услугу по охране информации, подвергаются потенциальным рискам как производственного, так и финансового характера по причине несанкционированного доступа к конфиденциальной информации.

По мнению Гранта Перди (Австралия) — соавтора ISO 31000, потратившего на изучение проблем управления рисками около полувека, многослойность подхода, сложившаяся в настоящее время, затрудняет возможность принимать решения по минимизации и купированию рисков. Причина такой ситуации кроется в отсутствии надежной базы знаний, а именно отсутствии единства в толковании самого термина «риск». Это может быть глагол «рисковать» или существительное, а также «шанс на успех» или последствия после реализации риска. Существует сорок значений термина «ISO» — это междуна-

[6] Кибермошенничество: портрет пострадавшего. Банк России. URL: https://www.cbr.ru/statistics/information_security/cyber_portrait/2024/

родная организация по стандартизации, но даже в ней не могут договориться, что означает «риск»». Как можно управлять тем явлением, единство в понимании которого отсутствует, продолжает свою мысль автор. Управление рисками — дорогостоящее мероприятие, отнимающее ресурсы, предназначенные для других функций компании, «создает ложное чувство безопасности, уверенности и невнимание к ресурсам, к тому, что люди должны делать, чтобы повысить качество принимаемых решений» (Восканян, 2020).

Результаты ранкинга Tadviser крупнейших поставщиков решений в сфере информационной безопасности в России по состоянию на декабрь 2024 г. на основе выручки за период 2021–2023 гг. представлены в таблице 3 и на рисунке 4.

Таблица 3

Ранкинг крупнейших поставщиков решений в сфере информационной безопасности в России (по выручке, млн руб.)

Table 3

Ranking of the largest suppliers of information security solutions in Russia (by revenue, million rubles)

Компания	2021	2022	2023	Темп прироста	
				2022–2021	2023–2022
Kaspersky	50784	51549	47736	1,5	–7,39
Газинформсервис	10508	15552	35985	48	131,4
Softline	20320	23428	34240	15,29	46,1
BI.ZONE	8971	17156	22820	91,2	33,01
Positive technologies	5803	13800	22213	137,8	60,96
SOLAR	6553	14400	17300	119,7	20,13
Innostage	4646	9501	14568	104,4	53,3
Get	6970	11300	14295	62,12	26,5
Infoteks	7290	8598	13737	17,9	59,8
Код безопасности	5854	6809	9200	16,3	35,11
Информзащита, системный интегратор	7282	6751	—	–7,29	—

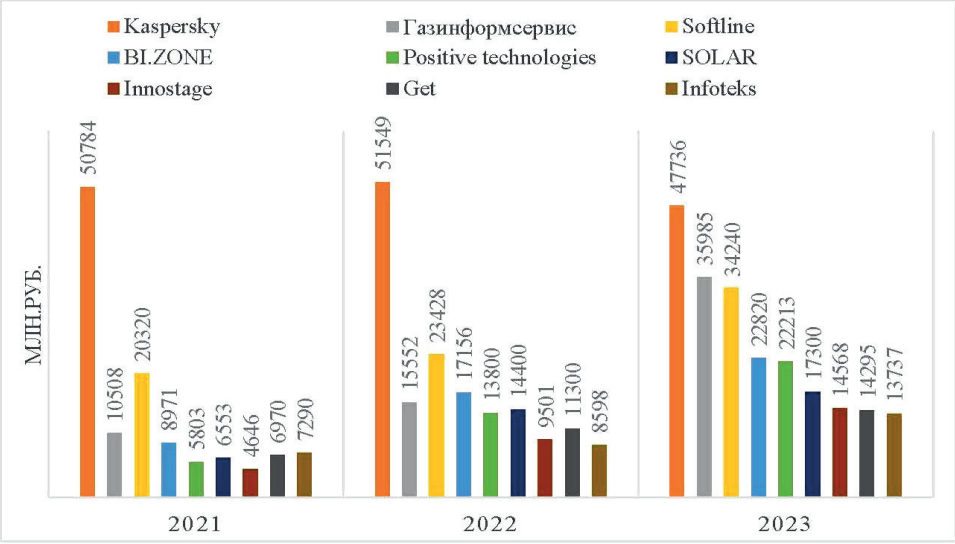

Рисунок 4 — Крупнейшие поставщики решений в сфере информационной безопасности в России (по выручке 2023 г., млн руб.).

Figure 4 — Largest providers of information security solutions in Russia (by revenue in 2023, million rubles).

Источник: составлено автором по данным TADVISER[7]

[7] Компания: BI. Zone_ (Безопасная_Информационная_Зона,_Бизон) // Tadviser. Государство. Бизнес. Технологии. URL: https://goo.su/awk5vu

Общая тенденция показателя выручки свидетельствует о том, что спрос на услуги в области информационной безопасности не снижается, а напротив, демонстрирует рост. С одной стороны, этот факт можно рассматривать как положительный аспект в управлении бизнес-структурами, с другой — как негативный, поскольку усиливается активность кибермошенников. Одни компании пополняют список заказчиков услуг по охране своих данных, обращаясь за защитой от несанкционированного доступа к информации, другие — расширяют перечень получаемых услуг по причине креативности желающих ее похитить.

Искажения, вуалирование и фальсификация информации финансовой отчетности

Причиной искажения может быть недостаточная компетентность сотрудников, которая выражается в отсутствии профессионального суждения при отражении фактов хозяйственной деятельности экономического субъекта. Эта проблема ложится на плечи отдела кадров и решается в процессе подбора кандидатов на соответствующую должность с учетом требований профессиональных стандартов.

Фальсификация данных отчетной информации — это преднамеренное искажение содержания отдельных отчетов, как правило, может совершаться группой лиц по предварительному сговору и ограничиваться «фильтрацией» на этапах внутреннего и внешнего аудита, а также административным или, в исключительных случаях, уголовным преследованием. Можно сказать, что данная схема «работы над ошибками» прозрачна, понятна и реализуется.

Вуалирование показателей отчетности юридического лица достигается умением правильного выбора норм из числа разрешенных для включения в содержание элементов учетной политики и согласуется с правильными кадровыми решениями.

Более сложной, на наш взгляд, остается борьба с фальсификацией информации, полученной с нарушением прав доступа, используемой в мошеннических целях. Несмотря на количество размещаемой в разных источниках информации, предостерегающей о возможных действиях мошенников, из года в год наблюдается рост количества пострадавших, а предпринимаемых усилий становится недостаточно.

Решение данной задачи возможно в первую очередь при соблюдении цифровой гигиены в цифровом поле. Цифровая гигиена в настоящий период времени представляет собой концептуальный подход, который посвящен поведению субъекта в интернет-пространстве, направлен на обеспечение безопасности и объясняет необходимость фильтрации информации.

Социальная инженерия на защите участников цифрового поля

Соблюдение цифровой гигиены должно стать одним из правил общественного поведения. Прививать навыки гигиены необходимо одновременно с повышением финансовой и цифровой грамотности участников цифрового обмена данными. Инструменты и методы социальной инженерии, к сожалению, в большей степени используются для несанкционированного использования информации с целью как финансового обогащения, так и финансовой поддержки действий, запрещенных законодательством. Возникает вопрос о возможности использования достижений в области психоанализа для предотвращения правонарушений. Специалист в области социальной инженерии в зависимости от цели исследует процессы как социального, так и межличностного характера для использования методов, изменяющих общественное поведение. В контексте борьбы с мошенническими действиями приемы социальной инженерии могут рассматриваться как базовый инструмент согласно теории Роско Паунда — инструмент, балансирующий интересы конфликтующих сторон посредством регулятивов (Меликовский, 2024). В данной концепции термин «инженерия» согласуется с функцией построения общественной структуры, которая способна, минимизируя конфликты, удовлетворять желания большего количества субъектов — участвующих в процессе обмена информацией и конфликтующих сторон. Имея социальный портрет пострадавшего, который представил Центральный банк, можно предположить возможность организации работы с различными социальными группами в зависимости от источника получаемой информации в рамках правового поля. Возможно расширить функции отдельных государственных институтов и частных компаний, выделяя в отдельный сегмент обязательное напоминание распространителем информации участникам (пользователям) о соблюдении цифровой гигиены и ответственности, а также о последствиях ее нарушения. Единственным пожеланием к создателям данного продукта должны быть простота и лаконичность информирования.

Выводы

Данные анализа причинно-следственных связей наличия и обращения в интернет-пространстве информации, не соответствующей ее базовой характеристике — достоверности, позволяют констатировать наличие замкнутого круга, разорвать который возможно в условиях системности в решении проблемы. В периметр проблем и способов их решения следует включить воспитание и повышение уровня развития навыков цифровой гигиены как поставщиков, так и пользователей информационного продук-

та; увеличение количества бизнес-структур, прибегающих к услугам IT-компаний за приобретением продуктов, снижающих вероятность информационной незащищенности; опережающие темпы развития защитных функций ИТ-решений в цифровом обмене данными; повышение уровня финансовой и цифровой грамотности участников информационного обмена; формирование концепции использования методов социальной инженерии для защиты участников цифрового поля.

СПИСОК ИСТОЧНИКОВ / LIST OF SOURCES

Восканян Е. Если риск-менеджмент — это ответ, то каким был вопрос? // Риск-менеджмент. Практика. 2020. № 1 [Voskanyan E. If Risk Management is the Answer, then What was the Question? *Risk-menedzhment. Praktika = Risk Management. Practice*. 2020;1 (In Russ.)].

Гапоненко А. Л., Орлова Т. М. Управление знаниями: как превратить знания в капитал. М. : ЭКСМО, 2008. С. 180 [Gaponenko A. L., Orlova T. M. Knowledge Management: How to Turn Knowledge into Capital. Moscow : EKSMO, 2008. P. 180 (In Russ.)].

Городов О. А. Информация как объект гражданских прав // Правоведение. 2001. № 5. С. 72–83 [Gorodov O. A. Information as an Object of Civil Rights. *Pravovedenie = Jurisprudence.* 2001;5:72–83 (In Russ.)].

Дубровский Е. Н. Информационно-обменные процессы — факторы социального развития // Проблемы социальной информатики. М. : Союз, 1996. Вып. 2. [Dubrovsky E. N. Information Exchange Processes — Factors of Social Development. *Problems of Social Informatics.* Moscow : Soyuz, 1996. Issue 2. (In Russ.)].

Меликовский А. А. Прагматическая философия права: Роско Паунд. В поисках теории для практики // Правовое государство: теория и практика. 2024. № 3. С. 30–38 [Melikovsky A. A. Pragmatic Philosophy of Law: Roscoe Pound. In Search of a Theory for Practice. *Pravovoe gosudarstvo: teoriya i praktika = The Rule of Law: Theory and Practice*. 2024;3:30–38 (In Russ.)].

Сократ. Я ничего не знаю / сост., предисл., коммент. А. В. Маркова. М. : АСТ, 2024. 320с. [Socrates. I know nothing / compiled, preface, commentary A. V. Markov. Moscow : AST, 2024. 320 p. (In Russ.)].

Шеннон К. Работы по теории информации и кибернетике. М. : Издательство иностранной литературы, 1963. 830 с. [Shannon K. Works on Information Theory and Cybernetics. Moscow : Izdatel'stvo inostrannoj literatury, 1963. 830 p. (In Russia)].