приоритет2030^
право для лидерства

МГЮА

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В УСЛОВИЯХ САНКЦИОННОГО ДАВЛЕНИЯ

ПРАВО УСТОЙЧИВОГО РАЗВИТИЯ

АНАЛИТИЧЕСКАЯ СПРАВКА

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ЮРИДИЧЕСКИЙ
УНИВЕРСИТЕТ ИМЕНИ О.Е. КУТАФИНА (МГЮА)»
(УНИВЕРСИТЕТ ИМЕНИ О.Е. КУТАФИНА (МГЮА))

АНАЛИТИЧЕСКАЯ СПРАВКА

«ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В УСЛОВИЯХ УСТОЙЧИВОГО РАЗВИТИЯ»

Москва, 2022

СПИСОК ИСПОЛНИТЕЛЕЙ

Доцент кафедры
международного частного
права, канд. юрид. наук _____ О.Ф. Засемкова

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

Директива № 95/46/ЕС – Директива Европейского союза № 95/46/ЕС от 24 октября 1995 г.

КСО – корпоративная социальная ответственность

ПДн – персональные данные

ФЗ «О персональных данных» - Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»

ФСТЭК – Федеральная служба по техническому и экспортному контролю

CCPA – Закон штата Калифорния «О защите частной жизни потребителей» 2018 г.

CISO – директор по информационной безопасности

CNIL – Французский регулятор по защите персональных данных

ENISA – Европейское агентство по информационной безопасности

ESG – экологичность, социальная ответственность, корпоративное управление

GDPR – Регламент Европейского Парламента и Совета ЕС № 2016/679 от 27 апреля 2016 г. «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС» (Общий Регламент о защите персональных данных)

ICO – Британский регулятор по защите персональных данных

ВВЕДЕНИЕ

Одной из ключевых задач, стоящих перед мировым сообществом в XXI веке, является переход к концепции устойчивого развития (*sustainable development*), предполагающей повышение благосостояния общества и одновременное снижение воздействия человека на окружающую среду, а также учет социальных и экономических проблем.

В сфере бизнеса данная концепция нашла свое отражение в сформулированных в 2004 году ESG-принципах, предполагающих учет трех основополагающих элементов («E» - «S» - «G»), свидетельствующих о вовлеченности компаний в решение глобальных экологических, социальных и управленческих проблем.

Как правило, дискуссии вокруг устойчивого развития и ESG-повестки фокусируются на таких факторах, как минимизация выбросов парниковых газов, достижение углеродной нейтральности, забота о сотрудниках, обеспечение гендерного разнообразия персонала и членов правления, улучшение качества корпоративного управления компанией.

Вопросы же кибербезопасности и защиты данных традиционно выносились за рамки ESG, будучи включенными в число «чисто технических» вопросов, которым компании уделяли незначительное внимание.

Однако в условиях стремительного развития информационных технологий и цифровизации практически всех сфер жизни современного общества, данный вопрос постепенно выходит на первый план, что обусловлено резким ростом числа кибератак и краж данных, затрагивающих в том числе критически важные инфраструктуры, и способных привести к катастрофическим последствиям.

В связи с этим, в последние годы все большее число компаний начинают включать информацию о способах защиты данных и обеспечения их конфиденциальности в отчеты об устойчивом развитии и ESG-политики.

1 УСТОЙЧИВОЕ РАЗВИТИЕ И ESG-ПРИНЦИПЫ

Одной из ключевых тенденций развития общества в XXI веке является переход к концепции устойчивого развития (от англ. sustainable development)[1], предполагающей преобразование мира по 17 основным направлениям – целям устойчивого развития (англ. sustainable development goals или SDG)[2], зафиксированным в принятой Генеральной Ассамблеей ООН Повестке дня в области устойчивого развития на период до 2030 года[3].

Рис. 1. Цели устойчивого развития ООН[4]

В сфере бизнеса данная концепция нашла свое отражение в

---

[1] Dentsu. White Paper. Устойчивое развитие & ESG. Гайд для маркетологов 2022. URL: https://assets-eu-01.kc-usercontent.com/296d8d4d-1c46-01bf-48d9-7c150d2fc3b5/c7d00561-f02b-4734-acd5-1b88ce215893/Dentsu%20Sustainability%20&%20ESG_2022.pdf (дата обращения: 10.10.2022); Жукова Е.В. Основные тенденции развития ESG-повестки: обзор в России и в мире // Вестник РЭУ им. Г.В. Плеханова. 2021. Т. 18. № 6 (120). С. 68-82; ESG-повестка как новый тренд российского бизнеса. URL: http://rapsinews.ru/incident_publication/20220321/307803134.html (дата обращения: 10.10.2022).

[2] KPMG. Время устойчивых: почему бизнес больше не может игнорировать ESG-повестку? URL: https://mustread.kpmg.ru/articles/vremya-ustoychivykh-pochemu-biznes-bolshe-ne-mozhet-ignorirovat-esg-povestku/ (дата обращения: 10.10.2022).

[3] Резолюция, принятая Генеральной Ассамблеей 25 сентября 2015 года. Преобразование нашего мира: Повестка дня в области устойчивого развития на период до 2030 года. URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=R (дата обращения: 10.10.2022).

[4] Цели в области устойчивого развития. URL: https://www.un.org/sustainabledevelopment/ru/sustainable-development-goals/ (дата обращения: 10.10.2022).

сформулированных в 2004 году ESG-принципах, предполагающих учет трех основополагающих элементов («E» - «S» - «G»), свидетельствующих о вовлеченности компаний в решение глобальных экологических, социальных и управленческих проблем[5] (Рис. 2).

Рис. 2. ESG-принципы

1.1 «E» - Environmental – экологичность и ответственное отношение к окружающей среде

В контексте устойчивого развития и ESG-принципов компонент «E» обозначает вопросы борьбы с климатическими изменениями, управления водными ресурсами, обращения с отходами, обеспечения биологического разнообразия, реализации «зеленых» проектов и снижения негативного воздействия хозяйственной деятельности на окружающую среду[6].

1.2 «S» – Social – социальная политика и социальная ответственность компаний

В контексте устойчивого развития и ESG-принципов термин «S» обозначает политику в области корпоративной социальной ответственности (далее – КСО), обеспечение социальной защищенности и профессионального

[5] Мажорина М.В. ESG-принципы в международном бизнесе и «устойчивые контракты» // Актуальные проблемы российского права. 2021. Т. 16. № 12(133). Декабрь. С. 187.
[6] Dentsu. White Paper. Устойчивое развитие & ESG. Гайд для маркетологов 2022. URL: https://assets-eu-01.kc-usercontent.com/296d8d4d-1c46-01bf-48d9-7c150d2fc3b5/c7d00561-f02b-4734-acd5-1b88ce215893/Dentsu%20Sustainability%20&%20ESG_2022.pdf (дата обращения: 10.10.2022).

развития сотрудников, обеспечение их гендерного равенства, работу с клиентами и реализацию планов по улучшению социально значимых показателей деятельности компании[7].

1.3 «G» - Governance – корпоративное управление

В контексте устойчивого развития и ESG-принципов термин «G» означает корпоративное управление, деловую репутацию компании, эффективность работы совета директоров, обеспечение транспарентности (прозрачности) информации, борьбу с коррупцией, систему управления рисками, защиту прав собственников, а также политику компании в отношении обеспечения соответствия раскрытия информации[8].

1.4 Значение ESG-принципов в современном мире

Изначально возникнув как добровольно принимаемые на себя компаниями обязательства, лишенные каких-либо юридических или рыночных рисков[9], ESG-принципы постепенно превратились в важные факторы, влияющие на возможность привлечения новых инвестиций и заемного финансирования[10], и оказывающие воздействие на репутацию компании.

Следуя данной тенденции, как потребители, так и инвесторы все чаще отдают предпочтение компаниям, придерживающимся ESG-принципов.

Так, по данным исследований, в 2020 году каждый четвертый доллар, инвестированный в экономику США, был направлен на развитие «устойчивых» компаний[11], а стоимость активов под управлением,

---

[7] Data Protection as a Corporate Social Responsibility. From Compliance to Sustainability to Generate Both Social and Financial Value. URL: https://www.maastrichtuniversity.nl/data-protection-corporate-social-responsibility (дата обращения: 10.10.2022).
[8] Dentsu. White Paper. Устойчивое развитие & ESG. Гайд для маркетологов 2022...
[9] Мажорина М.В. Указ. соч. С. 187-188.
[10] ESG-повестка как новый тренд российского бизнеса. URL: http://rapsinews.ru/incident_publication/20220321/307803134.html (дата обращения: 10.10.2022).
[11] 1 in 4 investing dollars are now going into ESG strategies. How to play it, according to Cowen. URL: https://www.cnbc.com/2021/03/18/sustainable-strategies-attract-1-in-4-investing-dollars.html (дата обращения: 10.10.2022).

соответствующим ESG-принципам, достигла 37,8 трлн. долл. США и продолжает увеличиваться[12].

На аналогичные тренды указывают и крупнейшие корпорации. Так, согласно прогнозам BlackRock, к 2028 году ответственные инвестиционные стратегии составят не менее 21 % от общих активов фонда, что позволит добиться существенного снижения рисков и обеспечить высокую доходность и лучшую устойчивость во время экономических кризисов, вызванных как пандемией коронавируса COVID-19, так и изменением геополитической обстановки в мире[13].

Аналогичная тенденция наблюдается применительно к потребителям, которые все чаще выбирают или бойкотируют бренды, исходя из их позиции по экологическим и социальным вопросам[14].

Как правило, дискуссии вокруг устойчивого развития и ESG-повестки фокусируются на таких факторах, как минимизация выбросов парниковых газов, достижение углеродной нейтральности, забота о сотрудниках, расширение разнообразия (в том числе гендерного) персонала и членов правления, улучшение качества корпоративного управления компанией[15].

Однако в условиях стремительного развития информационных технологий и цифровизации практически всех сфер жизни современного общества к ним добавляется вопрос об обеспечении информационной безопасности и защите персональных данных от несанкционированного доступа и иных нарушений[16], который приобретает все большее значение.

---

[12] KPMG. Время устойчивых: почему бизнес больше не может игнорировать ESG-повестку? URL: https://mustread.kpmg.ru/articles/vremya-ustoychivykh-pochemu-biznes-bolshe-ne-mozhet-ignorirovat-esg-povestku/ (дата обращения: 10.10.2022).

[13] BlacRock Takes Sustainable Investing Mainstream with Range of Low-Cost Sustainable Core ETFs. URL: https://ir.blackrock.com/news-and-events/press-releases/press-releases-details/2018/BlackRock-Takes-Sustainable-Investing-Mainstream-with-Range-of-Low-Cost-Sustainable-Core-ETFs/default.aspx (дата обращения: 08.10.2022).

[14] Edelman`s 2018 Earned Brand Study. October 2, 2018. URL: https://www.edelman.com/earned-brand (дата обращения: 08.10.2022).

[15] Сбер выпустил первый обзор ESG-трендов в России. URL: https://press.sber.ru/publications/sber-vypustil-pervyi-obzor-esg-trendov-v-rossii (дата обращения: 08.10.2022).

[16] Your ESGuide in 5: Finding the P for Privacy in ESG. URL: https://www.lexology.com/library/detail.aspx?g=8b1a2950-a343-4822-a751-06f19089cbf4 (дата обращения: 10.10.2022); Data Governance, Privacy and Trust – A Sweet Spot for ESG? URL: https://www.herbertsmithfreehills.com/insight/data-governance-privacy-and-trust-—-a-sweet-spot-for-esg (дата

2 ПРАВОВОЕ РЕГУЛИРОВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В РОССИИ И ЗАРУБЕЖНЫХ СТРАНАХ

2.1 Понятие персональных данных в России и зарубежных странах

Как отмечалось в разделе 1 настоящей Аналитической справки, в условиях развития новых технологий и многократного увеличения рисков кибератак и кражи данных, вопрос о защите ПДн от несанкционированного доступа приобретает особое значение.

В связи с этим, как на международном уровне, так и на уровне отдельных государств принимаются акты, направленные на защиту данных.

Особое место среди них занимает Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных 1981 г. (Конвенция 108)[17] и ее модернизированная версия (Конвенция 108+)[18], направленные на обеспечение прав и свобод граждан, включая право на неприкосновенность частной жизни и защиту данных, речь о которой пойдет в подразделе 2 раздела 2 настоящей Аналитической справки.

Аналогичным образом данный вопрос решается в законодательстве большинства государств, которые, тем не менее, по-разному подходят к определению ПДн (см. Таблицу 1).

Несмотря на некоторые различия, законодательство практически всех рассматриваемых государств (стран-членов ЕС, Великобритании, Канады,

---

обращения: 10.10.2022); ESG as the Next Frontier in Privacy and Data Governance: Moving Beyond Regulatory Compliance. URL: https://www.treasuryandrisk.com/2022/02/10/is-privacy-and-cybersecurity-the-next-frontier-for-esg-411-26421/c6b692ff-e718-4b36-a5f5-059ead10d552 (дата обращения: 10.10.2022); Are Privacy and Cybersecurity the Next Frontier for ESG? URL: https://www.treasuryandrisk.com/2022/02/10/is-privacy-and-cybersecurity-the-next-frontier-for-esg-411-26421/ (дата обращения: 10.10.2022); Facebook data privacy issue already identified by ESG investment screens. URL: https://www.investmentnews.com/facebook-data-privacy-issue-already-identified-by-esg-investment-screens-75033 (дата обращения: 10.10.2022); ESG and Privacy – a Foundation for Better Compliance? URL: https://www.alvarezandmarsal.com/insights/esg-and-privacy-foundation-better-compliance (дата обращения: 10.10.2022); Петрова Д.А. Правовые режимы защиты персональных данных в условиях цифровизации // Advances in Law Studies. 2020. Том 8. № 5. С. 79-85; Правовое регулирование искусственного интеллекта в условиях пандемии и инфодемии: монография / под общей ред. В.В. Блажеева, М.А. Егоровой. М.: Проспект, 2020 и др.

[17] Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных. По состоянию на 02.10.2022 г. участниками Конвенции являются 55 государств, включая РФ, для которой Конвенция вступила в силу 1 сентября 2013 г. // СЗ РФ. 03.02.2014. № 5. Ст. 419.

[18] Convention for the protection of individuals with regard to the processing of personal data. Convention 108+. URL: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf (дата обращения: 10.09.2022).

Японии, Сингапура и России) исходит из широкого подхода к определению ПДн, включая в их число сведения о физическом лице, позволяющие осуществить его идентификацию, как самостоятельно, так и в совокупности с другими данными. Причем в последние годы происходит расширение перечня сведений, включаемых в понятие ПДн, что обусловлено появлением новых видов информации, имеющей коммерческую ценность.

Иной подход к определению ПДн используется в США, где данный термин, равно, как и его единое определение, отсутствует как таковой. Вместо него в законодательстве, как правило, используется термин «персональная идентифицируемая информация» (*personally identifiable information*) либо «персональная информация» (*personal information*)[19].

При этом в США используется «секторальный» подход к защите такой информации, что предполагает принятие нормативных актов в различных сферах (государственном управлении, здравоохранении, сфере финансовых услуг и др.). Принятый же на федеральном уровне Закон о защите неприкосновенности частной жизни (US Privacy Act 1974[20]) имеет ограниченную сферу действия и регламентирует обработку персональной информации в отношении граждан США и лиц, постоянно проживающих на территории данного государства, исключительно федеральными органами исполнительной власти.

Помимо секторальных законов, регулирующих отдельные вопросы защиты ПДн, на уровне штатов действуют законы о защите частной жизни, которые также обязывают уведомлять об утечках данных и иных инцидентах с ними. Как правило, такие законодательные акты определяют персональную информацию посредством 2х основных критериев: 1) имени субъекта таких данных; 2) номера карточки социального страхования; номера водительского удостоверения; номера счета или банковской карты; либо любого иного идентификатора, используемого государством.

---

[19] Отчет 1 НИУ ВШЭ. URL: https://old.sk.ru/foundation/legal/p/03.aspx (дата обращения: 10.09.2022).
[20] US Privacy Act of 1974, as amended, 5 U.S.C. § 552a. URL: https://www.justice.gov/opcl/privacy-act-1974 (дата обращения: 10.09.2022).

Таблица 1 - Понятие персональных данных в России и зарубежных странах

№	Государство	Нормативный акт	Понятие персональных данных
1	Великобритания	Закон «О защите данных» (Data Protection Act), UK GDPR[21]	ПДн - любая информация, позволяющая прямо или косвенно осуществить идентификацию физического лица при помощи ссылки на его идентификационный номер, данные о местоположении, онлайн-идентификатор или один либо несколько специфических признаков, относящихся к физической, психологической, генетической, ментальной, экономической, культурной или социальной идентичности такого лица. Согласно разъяснениям[22], к числу ПДн относятся, в частности: имя и фамилия лица, его домашний адрес, адрес электронной почты, содержащий указание на имя и фамилию лица, номер удостоверения личности; данные о местоположении; IP-адрес; идентификатор cookie; данные о состоянии здоровья, позволяющие идентифицировать человека[23].
2	Европейский союз	Регламентом Европейского Парламента и Совета Европейского Союза № 2016/679 от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий регламент о защите персональных данных) (GDPR)[24]	

[21] DLI PIPER. Data Protection Laws of the World – United Kingdom. URL: https://www.dlapiperdataprotection.com/index.html?t=law&c=GB (дата обращения: 20.09.2022); Guide to the UK General Data Protection Regulation (UK GDPR). URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ (дата обращения: 20.09.2022).

[22] Article 29 Data Protection Party. Opinion 4/2007 on the concept of personal data. URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf (дата обращения: 20.09.2022); Отчет 1 НИУ ВШЭ. URL: https://old.sk.ru/foundation/legal/p/03.aspx (дата обращения: 20.09.2022).

[23] What is personal data? URL: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en (дата обращения: 20.09.2022).

[24] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (дата обращения: 10.09.2022).

3	Канада	Закон «О защите персональной информации и электронных документах» (PIPEDA) / Закон «О защите данных потребителей» (Consumer Privacy Protection Act), Закон «О суде по защите личной информации и данных» (Personal Information and Data Protection Tribunal Act)[25]	ПДн – любая информация об идентифицируемом физическом лице[26].
4	Сингапур	Закон «О защите персональных данных» (Personal Data Protection Act)[27], Руководящие принципы по обеспечению соблюдения законодательства о защите данных (Advisory Guidelines on Enforcement of the Data Protection Provisions)[28]	ПДн - сведения о физическом лице, живом или умершем (менее 10 лет назад), независимо от их достоверности и формы фиксации (электронной или нет), позволяющие идентифицировать такое лицо (как в случае, когда для этого достаточно таких данных, так и когда для этого требуются дополнительные сведения, к которым оператор имеет или может иметь доступ) [29]. Несмотря на достаточно широкое определение, из-под понятия ПДн выведены: 1) деловая контактная информация, включая ФИО, должность, рабочий номер телефона и адрес электронной почты, факса и т.д.; 2) сведения, собираемые государственными органами; 3) персональные данные, содержащиеся в записях, существующих более 100 лет[30].

[25] Canada: Understanding the Digital Charter Implementation Act, 2020. URL: https://www.mondaq.com/canada/privacy-protection/1027926/understanding-the-digital-charter-implementation-act-2020 (дата обращения: 21.08.2022).
[26] Personal Information Protection and Electronic Documents Act. URL: https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/page-1.html#h-416888 (дата обращения: 21.09.2022); DLI PIPER. Data Protection Laws of the World – Canada. URL: https://www.dlapiperdataprotection.com/index.html?t=definitions&c=CA&c2= (дата обращения: 20.09.2022).
[27] Personal Data Protection (Amendment) Act 2020. URL: https://sso.agc.gov.sg/Acts-Supp/40-2020/Published/20201210?DocDate=20201210 (дата обращения: 20.09.2022).
[28] Advisory Guidelines on Enforcement of the Data Protection Provisions (Issued 21 April 2016, Revised 1 February 2021). URL: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/Advisory-Guidelines-on-Enforcement-of-DP-Provisions-1-Feb-2021.pdf?la=en (дата обращения: 22.09.2022).
[29] Personal Data Protection Commission (Singapore). URL: https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act (дата обращения: 20.09.2022).
[30] Singapore – Data Protection Overview. URL: https://www.dataguidance.com/notes/singapore-data-protection-overview (дата обращения: 20.09.2022).

5	Штат Калифорния (США)	Закон «О защите персональных данных потребителей» (California Consumer Privacy Act)[31], Закон «О праве на конфиденциальность» (California Privacy Rights Act 2020)	ПДн – любая информация, идентифицирующая, описывающая, относящаяся, ассоциируемая или прямо либо косвенно связанная с конкретным потребителем, включая: - идентификаторы (имя, псевдоним, почтовый и электронный адрес, номер паспорта, карты социального страхования, водительского удостоверения, а также иные аналогичные данные); - подпись, описание физических данных лица, сведения о трудовом стаже, номере счетов, кредитных карт, информацию о состоянии здоровья; - сведения, могущие стать основанием для дискриминации лица (о расовой и национальной принадлежности, политических и религиозных взглядах и т.д.); - коммерческие сведения, включая данные о принадлежащей соответствующему лицу собственности, приобретенных товарах, услугах; - биометрические данные; - информацию об активности лица в сети Интернет; - сведения о геолокации; - аудио, электронные, визуальные и иные аналогичные данные; - информацию об образовании, трудовых отношениях, профессиональных интересах и т.д.
6	Япония	Закон о защите персональной информации (Act on the Protection of Personal Information)[32]	ПДн - персональная информация, которая содержится в базе данных оператора (например, в адресной книге

[31] California Consumer Privacy Act. URL: https://oag.ca.gov/privacy/ccpa#:~:text=The%20California%20Consumer%20Privacy%20Act,how%20to%20implement%20the%20law.&text=The%20right%20to%20opt%2Dout,of%20their%20personal%20information%3B%20and (дата обращения: 05.09.2022).

[32] DLI PIPER. Data Protection Laws of the World – Japan. URL: https://www.dlapiperdataprotection.com/index.html?t=definitions&c=JP&c2= (дата обращения: 20.09.2022).

			почтовой программы, оцифрованных данных визитных карточек и т.д.). При этом под персональной информацией понимается: 1) информация о живом физическом лице, позволяющая самостоятельно или путем простого обращения к иным сведениям идентифицировать его по таким данным, как имя, дата рождения или иное описание, а также 2) сведения о персональном идентифицирующем коде, охватывающем биометрические данные, номера документов и иные данные, являющиеся уникальными для данного человека и позволяющие идентифицировать его (например, номер паспорта или водительского удостоверения)[33].
7	Россия	ФЗ «О персональных данных»	ПДн - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу», включая информацию, представляющую собой результат преобразования таких данных в различного рода цифровые коды и иные идентификаторы (включая изображения граждан, используемые в информационных системах мониторинга поведения).

[33] Act on the Protection of Personal Information (APPI). URL: https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf (дата обращения: 20.09.2022).

2.2 Особенности защиты персональных данных в России и зарубежных странах

Одним из ключевых регуляторов в сфере защиты ПДн является принятая Советом Европы Конвенция о защите физических лиц при автоматизированной обработке персональных данных 1981 г. (Конвенция 108)[34] и ее модернизированная версия (Конвенция 108+)[35], согласно которым к числу основных стандартов защиты данных относятся:

1) наличие справедливой и законной основы сбора и обработки данных;

2) хранение и использование ПДн для определенных и законных целей;

3) адекватность, релевантность и соразмерность собираемых и подвергающихся автоматизированной обработке данных преследуемым такими действиями целям;

4) точность и своевременность обновления данных;

5) сохранение данных в форме, позволяющей осуществить идентификацию их субъектов, в течение только того периода, который необходим для достижения заявленных целей;

6) информирование субъектов о сборе и обработке касающихся их ПДн;

7) оценка воздействия, оказываемого такой обработкой, на права субъектов данных, до ее начала;

8) конфиденциальность собираемых и обрабатываемых данных, а также обеспечение их защиты, что особенно важно применительно к особым категориям персональных данных (таким, как информация о состоянии здоровья, расовой, религиозной, национальной принадлежности и др.)[36].

Аналогичные критерии предусмотрены в законодательстве различных стран, которые дополняют их мерами защиты ПДн и ответственности.

---

[34] Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных. Заключена в г. Страсбурге 28.01.1981 г. // Собрание законодательства РФ. 03.02.2014. № 5. Ст. 419.

[35] Convention for the protection of individuals with regard to the processing of personal data. Convention 108+. URL: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf (дата обращения: 10.10.2022).

[36] Засемкова О.Ф. Законодательство о защите персональных данных в цифровую эпоху: опыт России и зарубежных стран. В кн.: Актуальные проблемы права и экономики в ракурсе междисциплинарных научных исследований как формы международного сотрудничества / под общей ред. В.В. Блажеева, М.А. Егоровой. М., 2022. С. 126-141.

Таблица 2 – Стандарты защиты персональных данных в законодательстве России и зарубежных стран

№	Государство	Принципы обработки данных	Меры по защите данных	Меры ответственности за нарушение конфиденциальности
1	Великобритания	1) законность, справедливость и прозрачность; 2) наличие четко определенных законных целей обработки ПДн; 3) минимизация данных, то есть ограничение объема собираемой информации исключительно теми сведениями, которые необходимы для достижения заявленных целей; 4) точность; 5) ограничение срока хранения данных в форме, позволяющей идентифицировать их субъектов, только таким периодом, который необходим для достижения соответствующих целей;	Не содержит конкретных технических стандартов или мер по защите ПДн, лишь возлагая на контролеров и обработчиков данных обязанность предпринимать все необходимые технические и организационным меры для обеспечения уровня безопасности данных, соответствующего существующим рискам: 1) псевдонимизация и шифрование персональных данных; 2) обеспечение конфиденциальности, целостности, доступности и устойчивости систем обработки данных; 3) возможность своевременного восстановления доступа к персональным данным в случае физического или технического инцидента; 4) проведение регулярных тестов и оценок эффективности мер по обеспечению безопасности данных.	Штраф – до 4 % от годового оборота компании или 17,5 млн. фунтов стерлингов, в зависимости от того, какая сумма выше.
2	Европейский союз	6) целостность и конфиденциальность обрабатываемых	Меры организационного и технического характера: 1) обезличивание и шифрование ПДн;	Штраф – до 20 млн. евро или 4 % от мирового оборота компании-нарушителя, в зависимости от

		персональных данных; 7) принцип подотчетности.	2) обеспечение конфиденциальности, доступности и устойчивости систем и услуг, связанных с обработкой данных; 3) своевременное восстановление утраченного доступа к данным; 4) регулярное тестирование и оценка эффективности мер, принятых в целях обеспечения безопасности данных.	того, какая сумма больше.
3	Канада	Сбор, обработка и раскрытие ПДн допускаются только: 1) в тех целях, которые разумное лицо сочтет уместными в соответствующих обстоятельствах; 2) при наличии согласия субъекта данных, которое может быть отозвано; 3) в тех пределах и в течение такого срока, в каких это необходимо для достижения заранее установленной цели.	Меры организационного, технического, физического и административного характера, направленные на защиту информации от утраты, кражи, несанкционированного доступа, раскрытия, копирования, изменения и уничтожения, в то же время не устанавливая конкретных технических требований к осуществлению таких мер.	Штраф – до 5 % от годового оборота компании или 25 млн. канадских долл., в зависимости от того, какая сумма выше
4	Сингапур	1) необходимость обеспечения надлежащего уровня безопасности ПДн; 2) использование ПДн только в ограниченных целях;	Разумные меры по безопасности, а также уведомление об утечках данных уполномоченного органа (Комиссии по защите ПДн) и лиц, данные которых были раскрыты. Наряду с этим, Комиссия вправе:	Штраф – до 10 % от годового оборота компании (если сумма последнего превышает 10 млн. сингапурских долл. – 6,3 млн. евро) или 1 млн. сингапурских долл. (625 тыс. евро) в

		3) учет того факта, что организация занимается обработкой ПДн, раскрытие которых может привести к возникновению ущерба или иных неблагоприятных последствий для их субъектов, при расчете размера штрафа за их неправомерное раскрытие[37].	- прекратить сбор, использование или раскрытие персональных данных, осуществляемые с нарушением законодательства; - уничтожить персональные данные, полученные с нарушениями Закона; - вынести решение о разрешении или об отказе во внесении исправления в персональные данные.	зависимости от того, какая сумма больше[38].
5	Штат Калифорния (США)		Обязанности оператора ПДн: - по запросу потребителя предоставить информацию о собираемых и обрабатываемых данных, источниках их получения, целях обработки, категориях получателей данных, правах потребителей в отношении таких сведений и др.; - опубликовать политику конфиденциальности, раскрывающую категории собираемых данных, виды источников, из которых они собираются, категориях третьих лиц,	

[37] DLI PIPER. Data Protection Laws of the World – Singapore. URL: https://www.dlapiperdataprotection.com/index.html?t=definitions&c=SG&c2= (дата обращения: 20.09.2022).
[38] Singapore – Data Protection Overview. URL: https://www.dataguidance.com/notes/singapore-data-protection-overview (дата обращения: 22.09.2022).

			которым раскрывается такая информация и т.д.	
6	Япония	1) указание цели, для которой осуществляется сбор, обработка и использование информации; 2) минимизация собираемых данных, что предполагает недопустимость выхода за пределы того объема информации, который необходим для достижения соответствующей цели.		Штраф – до 500 тыс. йен. За неисполнение приказа Комиссии по защите ПДн: - для физических лиц – лишение свободы на срок до.1 года или штраф в размере до 1 млн. йен; - для юридических лиц – привлечение к ответственности должностных лиц или штраф в размере до 10 млн. йен[39].
7	Россия	1) принцип законности и наличия справедливой основы обработки персональных данных; 2) принцип минимальных данных, что предполагает ограничение обработки данных достижением строго определенных и законных целей; 3) принцип недопустимости объединения баз данных, содержащих персональные данные, обрабатываемые в целях, несовместимых между собой;	При обработке ПДн операторы обязаны предпринимать или обеспечивать принятие всех необходимых мер (правовых, организационных, технических), направленных на защиту ПДн «от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий, осуществляемых в отношении ПДн». Обеспечение безопасности данных может достигаться путем: - определения угроз безопасности ПДн при их обработке в информационных системах; - применения организационных и	Штраф за обработку ПДн, не совместимую с заявленными целями: - для физических лиц – от 2 до 6 тыс. руб.; - для должностных лиц – от 10 до 20 тыс. руб.; - для юридических лиц – от 60 до 100 тыс. руб. Шраф за обработку ПДн без согласия субъекта: - для физических лиц – от 6 до 10 тыс. руб.; - для должностных лиц – от 20 до 40 тыс. руб.; - для юридических лиц – от 30 до 150 тыс. руб.

[39] DLA Piper. Data Protection Laws of the World – Japan. URL: https://www.dlapiperdataprotection.com/index.html?t=enforcement&c=JP (дата обращения: 20.09.2022).

		4) принцип соответствия обрабатываемых данных заявленным целям такой обработки; 5) принцип точности, достаточности и актуальности обрабатываемых персональных данных и пр.	технических мер, направленных на обеспечение безопасности данных при их обработке в информационных системах, и необходимых для выполнения требований, предъявляемых к их защите; - применения средств защиты информации, прошедших процедуру оценки соответствия; - оценки эффективности принимаемых мер до ввода в эксплуатацию информационной системы; - учета машинных носителей персональных данных; - обнаружения фактов несанкционированного доступа к ПДн и принятия соответствующих мер; - восстановления персональных данных, которые были модифицированы или уничтожены ввиду несанкционированного доступа к ним со стороны третьих лиц; - установления правил доступа к персональным данным, обрабатываемым в информационной системе; - контроля за принимаемыми мерами и уровнем защищенности информационных систем.	

Как видно из Таблицы 2, в настоящее время в мире существует 2 основных подхода к определению оснований для обработки данных.

Если на территории стран-членов Европейского союза для этого необходимы соответствующие законные основания (принцип запрета обработки данных по умолчанию), то законодательство США напротив исходит из того, что такая обработка разрешена по умолчанию (за исключением случаев, когда речь идет об особых категориях данных).

В то же время в Сингапуре принят промежуточный подход, предусматривающий возможность констатации подразумеваемого согласия субъекта на обработку его данных.

При этом независимо от того, о какой стране идет речь, необходимыми условиями для осуществления обработки данных являются:

а) сбор, хранение и использование данных исключительно для определенных и законных целей;

б) адекватность, релевантность и соразмерность собираемых и подвергающихся обработке данных преследуемым такими действиями целям;

в) точность и своевременность обновления данных;

г) сохранение данных в форме, позволяющей осуществить идентификацию их субъектов, в течение только того периода, который необходим для заявленных целей;

д) информирование субъектов о факте сбора и обработки касающихся их персональных данных;

е) оценка воздействия, оказываемого такой обработкой на права субъектов данных, до ее начала;

ж) конфиденциальность собираемых и обрабатываемых данных, а также обеспечение их защиты.

За нарушение указанных условий в законодательстве всех рассматриваемых государств установлена ответственность, максимальный размер которой (согласно GDPR) достигает 4 % от мирового оборота компании или 20 млн. евро в зависимости от того, какая сумма больше.

3 ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В УСЛОВИЯХ УСТОЙЧИВОГО РАЗВИТИЯ

Учитывая значимость вопроса о кибербезопасности и защите ПДн, а также размеры штрафов, установленные за нарушение соответствующего законодательства, все большее число компаний начинает уделять этому вопросу существенное значение.

Во многом этому способствует и многократное увеличение числа кибератак, происходящих в последние годы, а также рост наносимого ими ущерба. Так, по данным IBM/Ponemon Institute, в 2021 году средний ущерб от утечки ПДн составил 4,24 млн. долл. США, что на 10 % больше, чем в 2019 году (3,86 млн. долл. США).

Участились кибератаки и на критически важную инфраструктуру (такую как добыча нефти и газа, химическое производство, морские системы и т.д.), что создает риск возникновения пожаров, взрывов, выбросов опасных веществ и прочих негативных, а зачастую и опасных последствий.

Как следствие, кибербезопасность и защита ПДн из «чисто технических» вопросов, которым компании традиционно уделяли незначительное внимание, постепенно превращаются в вопросы первостепенной важности, что подтверждается их включением в число ESG-факторов, привлекающих все больше внимания как со стороны инвесторов[40], так и со стороны широкой общественности.

Так, по данным ежегодного отчета Комиссара по информации Великобритании (UK Information Commissioner), около 77 % респондентов заявили о принципиальной важности для них вопроса защиты их

[40] The Role of Data Privacy and Security in ESG (Environmental, Social, Governance) https://www.ardentprivacy.ai/the-role-of-data-privacy-and-security-in-esg-environmental-social-governance/ (дата обращения: 08.10.2022).

персональных данных[41]. Аналогичные цифры показывают данные и других опросов[42].

Не менее значим данный вопрос и для инвесторов, что подтверждают данные опроса, проведенного RBC Global Asset Management, согласно которому 15 % респондентов назвали кибербезопасность / защиту ПДн наиболее серьезной проблемой ESG, еще 10 % считают это важным вопросом[43].

При этом независимо от того, предполагает ли деятельность компании управление глобальной сетью, вопрос о конфиденциальности (англ. *privacy*) и защите данных все чаще будет попадать в фокус устойчивого развития и ESG-повестки.

По прогнозам экспертов, всего за 4 года в мире будет создано более 175 трлн. гигабайт новых данных[44], а их защита постепенно приобретет ключевое значение в контексте ESG-повестки. Данный тренд подтверждается ростом корпоративных комментариев по вопросам конфиденциальности на 920 % за последние 5 лет[45], а также рядом громких дел, наглядно продемонстрировавших влияние недостаточной защиты данных на стоимость компании и ее репутацию.

Так, скандал с компанией Cambridge Analytica, незаконно собравшей данные более 87 млн. пользователей социальной сети Facebook, повлек падение стоимости акций последней почти на 1/5, а также привел к пересмотру несколькими фондами, придерживающимися принципов ESG, своих деловых

---

[41] Information Commissioner`s Annual Report and Financial Statements 2020-21. July 2021. HC354. URL: https://ico.org.uk/media/about-the-ico/documents/2620166/hc-354-information-commissioners-ara-2020-21.pdf (дата обращения: 08.10.2022).
[42] Privacy, Data Protection is Top ESG Concern Among Consumers. URL: https://blog.451alliance.com/privacy-data-protection-is-top-esg-concern-among-consumers/ (дата обращения: 08.10.2022).
[43] RBC Global Asset Management. 2021. URL: https://www.rbcgam.com/documents/en/other/esg-key-findings.pdf (дата обращения: 08.10.2022).
[44] IDC: Expect 175 zettabytes of data worldwide by 2025. URL: https://www.networkworld.com/article/3325397/idc-expect-175-zettabytes-of-data-worldwide-by-2025.html (дата обращения: 08.10.2022).
[45] Data Privacy & ESG. URL: https://redcloveradvisors.com/2021/05/21/data-privacy-esg-2/ (дата обращения: 05.10.2022).

связей с компанией[46]. А после публикации в Wall Street Journal обвинений в адрес компании, Facebook снова подверглась пристальному вниманию со стороны инвесторов, ориентированных на ESG[47].

Не меньший ущерб нарушение безопасности данных, поставившее под угрозу личную информацию более чем 1 млрд. пользователей, нанесло компании Yahoo, стоимость которой снизилась на 350 млн. долл. США[48].

Учитывая значимость вопросов обеспечения конфиденциальности и защиты ПДн в современном мире, данные вопросы постепенно находят свое отражение во всех элементах ESG (Рис. 3).

Рис. 3. Защита данных в контексте ESG-принципов

3.1 Защита персональных данных и информационная безопасность в контексте экологии и ответственного отношения к окружающей среде

[46] Socially responsible investors reassess Facebook ownership. URL: https://www.reuters.com/article/us-facebook-cambridge-analytica-funds-an-idUSKBN1GV318 (дата обращения: 05.10.2022).
[47] Your ESG fund might be invested in Facebook – and it highlights a major issue with sustainable investing. URL: https://www.cnbc.com/2021/10/26/your-esg-fund-might-be-invested-in-facebook.html (дата обращения: 05.10.2022).
[48] Verizon Will Pay $350 Million +Less for Yahoo. URL: https://www.nytimes.com/2017/02/21/technology/verizon-will-pay-350-million-less-for-yahoo.html (дата обращения: 03.10.2022).

Как отмечалось в подразделе 1 раздела 1 настоящей Аналитической справки, в контексте ESG экологический компонент - «E» -, как правило, обозначает борьбу с изменением климата, реализацию «зеленых» проектов и снижение негативного воздействия хозяйственной деятельности на окружающую среду.

Однако не меньшее влияние на экологию оказывает сбор, хранение и обработка огромных массивов данных, которые требуют использования значительных объемов энергии и приводят к выбросам до 3,9 % от всех мировых выбросов парниковых газов[49].

В целях решения данной проблемы компании, придерживающиеся ESG-принципов, придерживаются принципа минимизации, то есть собирают лишь те данные, которые необходимы для достижения заявленной цели, и ограничивают сроки их хранения, что позволяет снизить негативное воздействие на окружающую среду[50].

Не менее важную роль в защите окружающей среды играет использование энергосберегающих способов строительства и эксплуатации центров обработки данных и серверных центров.

3.2 Защита персональных данных и информационная безопасность в контексте социальной политики и социальной ответственности компаний

В контексте ESG-повестки социальный компонент – «S» - обозначает политику в области корпоративной социальной ответственности (КСО), обеспечение социальной защищенности сотрудников и реализацию планов по улучшению социально значимых показателей деятельности компании.

Наряду с этим, речь идет о защите прав человека, к числу которых

[49] The climate impact of ICT: A review of estimates, trends and regulations. URL: https://arxiv.org/ftp/arxiv/papers/2102/2102.02622.pdf (дата обращения: 09.10.2022).
[50] Dentsu. White Paper. Устойчивое развитие & ESG. Гайд для маркетологов 2022. URL: https://assets-eu-01.kc-usercontent.com/296d8d4d-1c46-01bf-48d9-7c150d2fc3b5/c7d00561-f02b-4734-acd5-1b88ce215893/Dentsu%20Sustainability%20&%20ESG_2022.pdf (дата обращения: 09.10.2022).

относится и право на неприкосновенность частной жизни и защиту данных[51] , предусмотренные рядом международных документов (например, Всеобщей декларацией прав человека 1948 г.[52], Европейской конвенцией о правах человека 1950 г.[53], Хартией Европейского Союза об основных правах[54] и др.). Применительно к ESG-повестке это означает необходимость осознания компаниями своей социальной ответственности за защиту ПДн сотрудников и клиентов, что требует принятия мер по противодействию утечкам данных, которые оказывают значительное влияние как на репутацию компании, так и на доверие к ней потребителей, которые, в свою очередь, все чаще требуют усиления контроля над сбором, использованием их конфиденциальной личной информации и ограничения ее объема лишь тем необходимым минимумом, который требуется для достижения поставленной цели.

Соответствующие требования закреплены в большинстве законодательных актов, посвященных защите ПДн (см. раздел 2 настоящей Аналитической справки). Особое место среди них занимает Общий регламент о защите персональных данных (GDPR), который закрепляет требование минимизации объема собираемых данных, а также устанавливает требование подотчетности и ответственности компаний за обеспечение надлежащего мониторинга и контроля за соблюдением обязательств в области конфиденциальности[55].

Аналогичные требования закреплены в ФЗ «О персональных данных», согласно которому оператор ПДн обязан принимать все необходимые меры по защите ПДн, препятствующие получению неправомерного или случайного

---

[51] Why is Cybersecurity Important to ESG Frameworks? URL: https://www.jpmorgan.com/insights/research/why-is-cybersecurity-important-to-esg (дата обращения: 09.10.2022).

[52] Всеобщая декларация прав человека. Принята резолюцией 217 А (III) Генеральной Ассамблеи ООН от 10 декабря 1948 г. URL: https://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml (дата обращения: 09.10.2022).

[53] Европейская конвенция по правам человека. Измененная и дополненная Протоколами № 11, 14 и 15 в сопровождении Дополнительного протокола и Протоколов № 4, 6, 7, 12, 13 и 16. URL: https://www.echr.coe.int/documents/convention_rus.pdf (дата обращения: 09.10.2022).

[54] Хартия Европейского Союза об основных правах. URL: https://eulaw.ru/treaties/charter/ (дата обращения: 09.10.2022).

[55] The EU General Data Protection Regulation. Questions and Answers. URL: https://www.hrw.org/news/2018/06/06/eu-general-data-protection-regulation (дата обращения: 09.10.2022).

доступа, уничтожению, изменению, блокированию, распространению и совершению иных неправомерных действий в отношении таких данных со стороны третьих лиц.

Особую актуальность вопрос обработки и использования ПДн приобретает в компаниях, использующих искусственный интеллект или какую-либо иную автоматизированную систему принятия решений, которые оказывают воздействие на людей (например, для определения того, следует ли предоставлять лицу кредит, или выявления потенциального мошенничества со стороны претендентов на получение пособия). В таком случае политика компании (помимо обеспечения кибербезопасности и защиты ПДн) должна быть направлена на обнаружение и предотвращение возможных уязвимостей и предвзятостей, которые могут повлиять на получаемый в результате использовании соответствующей системы результат.

3.3 Защита персональных данных и информационная безопасность в контексте корпоративного управления

В контексте ESG-повестки компонент корпоративного управления - «G» - означает обеспечение транспарентности (прозрачности) информации, борьбу с коррупцией, а также политику компании в отношении обеспечения соответствия раскрытия информации[56]. Наряду с этим, компании должны обеспечивать соблюдение применимого законодательства, регулирующего сбор и обработку персональных данных[57] (включая требование подотчетности и ответственности компании за обеспечение мониторинга и контроля за выполнение обязательств в области конфиденциальности)[58] и устанавливать разумные стандарты их защиты.

---

[56] Dentsu. White Paper. Устойчивое развитие & ESG. Гайд для маркетологов 2022. URL: https://assets-eu-01.kc-usercontent.com/296d8d4d-1c46-01bf-48d9-7c150d2fc3b5/c7d00561-f02b-4734-acd5-1b88ce215893/Dentsu%20Sustainability%20&%20ESG_2022.pdf (дата обращения: 10.10.2022).

[57] Your ESGuide in 5: Finding the P for Privacy in ESG. URL: https://viewpoints.reedsmith.com/post/102hhbt/your-esguide-in-5-finding-the-p-for-privacy-in-esg (дата обращения: 10.10.2022).

[58] ESG and Privacy – a Foundation for Better Compliance? URL: https://www.alvarezandmarsal.com/insights/esg-and-privacy-foundation-better-compliance (дата обращения: 01.10.2022).

Несоблюдение указанных требований не только сигнализирует инвесторам, заботящимся о соблюдении ESG-принципов, о небрежном отношении руководства компании к выполнению возложенных на нее обязательств, но и влечет возникновение репутационных рисков и создает угрозу привлечения компании к ответственности.

Так, нарушение британской версии GDPR может привести к различного рода штрафам, размер которых достигает 4 % от мирового оборота компании или 17,5 млн. фунтов стерлингов в зависимости от того, какая сумма больше. Аналогичные суммы штрафов предусмотрены самим GDPR – до 4 % от мирового оборота компании или 20 млн. евро, который может привести и к привлечению уголовной ответственности за несоблюдение законодательства о защите данных или несанкционированное раскрытие соответствующих данных.

Как правило, соответствующие меры ответственности сочетаются с требованием о незамедлительном принятии мер, направленных на устранение нарушений, что может повлечь за собой значительные операционные расходы и лишить компанию возможности использования собранных данных. Указанные обстоятельства, очевидно, нанесут ущерб репутации компании, приведут к потере ее инвестиционной привлекательности и, соответственно, снижению прибыли.

***

Учитывая важную роль обеспечения кибербезопасности и защиты данных в контексте ESG, некоторые рейтинговые агентства и регуляторы (такие, как SustainAnalytics, Morgan Stanley Capital International`s Emerging Markets Index и Совет по стандартам устойчивого развития (SASB)) включили данные вопросы в число критериев, оцениваемых при присуждении компании соответствующего рейтинга[59].

[59] Connect privacy with ESG to drive broader business success. URL: https://www.ey.com/en_ca/sustainability/connect-privacy-with-esg-to-drive-broader-business-success (дата обращения: 01.10.2022).

Так, по оценке агентства SustainAnalytics, из 7 крупнейших технологических гигантов, таких как Amazon, Apple, Facebook, Google, Microsoft, Netflix и Twitter, действенная модель управления данными и обеспечения конфиденциальности принята лишь в одной – Apple[60]. Используемые же такими технологическими гигантами, как Amazon и Facebook, бизнес-модели и политики управления данными недостаточно надежны и подвержены значительному числу рисков и уязвимостей, что оказывает влияние на рейтинг данных компаний, а, соответственно, и на их инвестиционную привлекательность.

Повышенное внимание к ответственному управлению данными положило начало тенденции включения информации о способах их защиты и обеспечения конфиденциальности в ESG-политики или отчеты об устойчивом развитии, публикуемые многими компаниями.

Так, компания Mastercard Inc. относит конфиденциальность и защиту данных к числу проблем устойчивого развития[61].

Политике защиты данных в контексте ESG уделяет внимание и Национальный банк Катара, который включает соответствующий вопрос в свою социальную политику[62].

Аналогичного подхода придерживается компания Verizon Communications Inc., в которой:

- была принята политика защиты данных;

- при разработке продуктов, систем и иных инициатив проводится оценка соблюдения конфиденциальности;

- внедрен сторонний процесс управления рисками, фокусирующийся на поставщиках и партнерах компании, имеющих высокий риск нарушения

[60] Why Data Privacy Is an ESG Issue. URL: https://www.theimpactivate.com/why-data-privacy-is-an-esg-issue/ (дата обращения: 01.10.2022).
[61] ESG Data Privacy and Protection. URL: https://www.alpha-sense.com/blog/data-privacy-esg/ (дата обращения: 01.10.2022).

[62] ESG Data Privacy and Protection. URL: https://www.alpha-sense.com/blog/data-privacy-esg/ (дата обращения: 10.10.2022).

конфиденциальности;

- назначен сотрудник по вопросам конфиденциальности;

- предпринимаются меры по обеспечению конфиденциальности детей в сети. Интернет и др.[63]

Схожим образом данный вопрос решается компанией Blackstone, которая также включила указанные вопросы в состав своей ESG-политики, а именно в раздел, посвященный G-компоненту (то есть вопросам корпоративного управления)[64].

Вопросы обеспечения конфиденциальности и защиты данных рассматриваются в отчетах и политиках и других компаний (например, Verisk Analytics Inc., Aristocrat Leisure Ltd., Equifax и др.)[65].

[63] Verizon. Digital responsibility. Privacy and data protection. URL: https://www.verizon.com/about/sites/default/files/esg-report/2019/social/digital-responsibility/privacy-and-data-protection.html (дата обращения: 10.10.2022).

[64] Blackstone. An Integrated Approach to ESG. URL: https://www.blackstone.com/wp-content/uploads/sites/2/2021/11/2021-ESG-Update_An-Integrated-Approach-to-ESG.pdf (дата обращения: 10.10.2022).

[65] ESG Data Privacy and Protection. URL: https://www.alpha-sense.com/blog/data-privacy-esg/ (дата обращения: 10.10.2022).

4 МЕРЫ ПО ЗАЩИТЕ ДАННЫХ И ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ УСТОЙЧИВОГО РАЗВИТИЯ

Как отмечалось в разделе 3 настоящей Аналитической справки, в настоящее время компании, придерживающиеся ESG-принципов и стандартов ответственного ведения бизнеса, должны принимать меры по обеспечению конфиденциальности собираемой ими информации и защите ее от несанкционированного доступа и разглашения.

Как видно из приведенных в разделе 3 настоящей Аналитической справки примеров, одним из наиболее эффективных способов обеспечения кибербезопасности и защиты данных, является включение этих вопросов во все внутренние процессы компании на всех уровнях, что может достигаться путем внедрения данных аспектов в ESG-политику компании.

При этом необходимо предпринять следующие основные действия (Таблица 3).

Таблица 3 – Основные меры по обеспечению конфиденциальности и защите ПДн

№	Наименование меры	Суть предлагаемой меры
1	Создание структуры обеспечения конфиденциальности и управления данными	Предполагает принятие политики либо стратегии обеспечения конфиденциальности и защиты персональных данных, что позволит выявить существующие и потенциальные риски и уязвимости, связанные со сбором, обработкой, управлением ПДн, и оценить принимаемые компанией меры на предмет их эффективности и соответствия требованиям применимого законодательства и отраслевых стандартов и принципов (например, NIST privacy framework, ISO 27701). Указанные меры должны приниматься на всех стадиях жизненного цикла данных (начиная от сбора и заканчивая их хранением и уничтожением).
2	Принятие мер по активному мониторингу практики	Действующие нормативные правовые акты (например, ФЗ «О защите персональных данных» и GDPR) требуют не только соблюдения указанных в них требований, но и принятия мер по активному

	конфиденциальности и управления данными	мониторингу практики конфиденциальности и управления данными, что позволяет своевременно выявлять и устранять возникающие угрозы и нарушения. Для этого многие компании назначают специального сотрудника, отвечающего за вопросы обеспечения конфиденциальности и защиты данных, а также внедряют отраслевые стандарты безопасности и конфиденциальности, способные защитить компанию от утечки данных и кибератак.
3	Проведение регулярных проверок кибербезопасности	Рекомендуется на регулярной основе проводить проверки политик и систем конфиденциальности и кибербезопасности как внутри компании, так и совместно с ее деловыми партнерами, продавцами, поставщиками и пр.
4	Разработка показателей конфиденциальности, кибербезопасности и управления данными, которые позволят отслеживать процесс достижения поставленных целей ESG в отношении таких данных	Сделав конфиденциальность и управление данными оцениваемым компонентом ESG, руководство компании получит представление о проблемах, возникающих в данной области, а также в процессе их устранения. Как правило, такие показатели определяются исходя из выявленных компанией рисков, ее внутренних потребностей и отрасли, в которой она работает. На практике большинство компаний относит к числу таковых наличие сертификатов информационной безопасности, статистику зафиксированных нарушений, уровень инвестиций и конфиденциальность и защиту данных и т.д.
5	Установить конфиденциальность данных по умолчанию (англ. by default)	Указанное требование предусмотрено в GDPR, а также стандарте ISO 31700 «Защита потребителей: конфиденциальность по умолчанию для потребительских товаров и услуг». Согласно данным положениям, компании, осуществляющие сбор, обработку, использование и хранение данных, должны принимать соответствующие технические и организационные меры, направленные на эффективное внедрение принципов защиты данных.
6	Создать систему подотчетности	Предполагает назначение сотрудника, ответственного за защиту данных и реализацию программ управления конфиденциальностью. Создание такой системы позволит получить ценную информацию о проблемах компании, связанных с кибербезопасностью, и привлечь к ответственности бизнес-подразделения, систематически допускающие нарушения правил безопасности данных.
7	Принять стратегию минимизации собираемых данных	Предполагает соблюдение требований, установленных применимым законодательством (например, Федеральным законом «О защите

		персональных данных» и GDPR) в части ограничения объемов собираемой информацией лишь теми сведениями, которые необходимы для достижения соответствующей цели, что, в свою очередь, будет способствовать ограничению негативного воздействия деятельности компании на окружающую среду за счет сокращения энергии, используемой серверами для обработки и хранения данных и снижения объема электронных отходов, образующихся при утилизации электронного оборудования.
8	Раскрыть информацию в отношении этики данных и кибербезопасности	Выполнение указанных действий продемонстрирует клиентам, инвесторам и другим заинтересованным лицам, что при сборе, хранении, обработке и использовании данных, компания соблюдает этические нормы, требования применимого законодательства, а также принимает необходимые для защиты соответствующих данных меры. Наряду с этим, компаниям рекомендуется производить оценку объема и качества раскрытия информации, касающейся конфиденциальности данных, рисков и уязвимостей, что предполагает предоставление акционерам дополнительной информации о механизмах, политиках и процессах управления конфиденциальностью и защитой ПДн. Речь идет об оценке такой информации, как: - расходы, понесенные в результате нарушений информационной безопасности; - время, прошедшее с момента последнего нарушения; - сертификация по определенным стандартам информационной безопасности; - наличие программ подготовки и переподготовки сотрудников по направлению информационной безопасности.

ЗАКЛЮЧЕНИЕ

Проведенное исследование позволило сформулировать следующие основные выводы:

1. В настоящее время компании, придерживающиеся ESG-принципов и стандартов ответственного ведения бизнеса, должны принимать меры по обеспечению конфиденциальности собираемой ими информации и защите ее от несанкционированного доступа и разглашения.

2. Повышенное внимание к ответственному управлению данными положило начало тенденции включения информации о способах их защиты и обеспечения конфиденциальности в отчеты об устойчивом развитии, публикуемые многими компаниями.

3. Соответствующие меры могут быть также интегрированы в ESG-политику компании. При этом необходимо:

- создать структуру обеспечения конфиденциальности и управления данными;

- принять меры по активному мониторингу практики конфиденциальности и управления данными;

- на регулярной основе проводить проверки кибербезопасности;

- разработать показатели конфиденциальности и управления данными, позволяющие отслеживать уязвимости и прогресс в их устранении;

- установить конфиденциальность по умолчанию (by default);

- создать внутреннюю систему подотчетности;

- принять стратегию минимизации собираемых данных.

4. Эффективная политика конфиденциальности и управления данными может улучшить репутацию компании, защитить ее от финансовых рисков, которые могут возникнуть в случае утечки персональных данных, а также повысить ее инвестиционную привлекательность.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Международные договоры, акты ЕС и иные международные документы:

1. Всеобщая декларация прав человека. Принята резолюцией 217 А (III) Генеральной Ассамблеи ООН от 10 декабря 1948 г. URL: https://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml (дата обращения: 09.10.2022).

2. Европейская конвенция по правам человека. Измененная и дополненная Протоколами № 11, 14 и 15 в сопровождении Дополнительного протокола и Протоколов № 4, 6, 7, 12, 13 и 16. URL: https://www.echr.coe.int/documents/convention_rus.pdf (дата обращения: 09.10.2022).

3. Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных. Заключена в г. Страсбурге 28.01.1981 г. // Собрание законодательства РФ. 03.02.2014. № 5. Ст. 419.

4. Хартия Европейского Союза об основных правах. URL: https://eulaw.ru/treaties/charter/ (дата обращения: 09.10.2022).

5. Резолюция, принятая Генеральной Ассамблеей 25 сентября 2015 года. Преобразование нашего мира: Повестка дня в области устойчивого развития на период до 2030 года. URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=R (дата обращения: 10.10.2022).

6. Цели в области устойчивого развития. URL: https://www.un.org/sustainabledevelopment/ru/sustainable-development-goals/ (дата обращения: 10.10.2022).

7. Convention for the protection of individuals with regard to the processing of personal data. Convention 108+. URL: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIB

E/DV/2018/09-10/Convention_108_EN.pdf (дата обращения: 10.10.2022).

8. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (дата обращения: 10.09.2022).

9. Article 29 Data Protection Party. Opinion 4/2007 on the concept of personal data. URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf (дата обращения: 20.09.2022);

Национальное законодательство РФ и зарубежных стран, отчеты и комментарии к законодательству:

10. Федеральный закон от 27.07.2006 г. (ред. от 14.07.2022) № 152-ФЗ «О персональных данных» // СЗ РФ. 31.07.2006. № 31 (1 ч.). Ст. 3451.

11. Act on the Protection of Personal Information (APPI). URL: https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf (дата обращения: 20.09.2022).

12. California Consumer Privacy Act. URL: https://oag.ca.gov/privacy/ccpa#:~:text=The%20California%20Consumer%20Privacy%20Act,how%20to%20implement%20the%20law.&text=The%20right%20to%20opt%2Dout,of%20their%20personal%20information%3B%20and (дата обращения: 05.09.2022).

13. Personal Data Protection (Amendment) Act 2020. URL: https://sso.agc.gov.sg/Acts-Supp/40-2020/Published/20201210?DocDate=20201210 (дата обращения: 20.09.2022).

14. Personal Information Protection and Electronic Documents Act. URL: https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/page-1.html#h-416888 (дата обращения: 21.09.2022).

15. US Privacy Act of 1974, as amended, 5 U.S.C. § 552a. URL: https://www.justice.gov/opcl/privacy-act-1974 (дата обращения: 10.09.2022).

16. Advisory Guidelines on Enforcement of the Data Protection Provisions (Issued 21 April 2016, Revised 1 February 2021). URL: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/Advisory-Guidelines-on-Enforcement-of-DP-Provisions-1-Feb-2021.pdf?la=en (дата обращения: 22.09.2022).

17. Canada: Understanding the Digital Charter Implementation Act, 2020. URL: https://www.mondaq.com/canada/privacy-protection/1027926/understanding-the-digital-charter-implementation-act-2020 (дата обращения: 21.08.2022).

18. Guide to the UK General Data Protection Regulation (UK GDPR). URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ (дата обращения: 20.09.2022).

19. Information Commissioner`s Annual Report and Financial Statements 2020-21. July 2021. HC354. URL: https://ico.org.uk/media/about-the-ico/documents/2620166/hc-354-information-commissioners-ara-2020-21.pdf (дата обращения: 08.10.2022).

20. Personal Data Protection Commission (Singapore). URL: https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act (дата обращения: 20.09.2022).

Научная литература:

21. Жукова Е.В. Основные тенденции развития ESG-повестки: обзор в России и в мире // Вестник РЭУ им. Г.В. Плеханова. 2021. Т. 18. № 6 (120).

22. Засемкова О.Ф. Законодательство о защите персональных данных в цифровую эпоху: опыт России и зарубежных стран. В кн.: Актуальные проблемы права и экономики в ракурсе междисциплинарных научных исследований как формы международного сотрудничества / под общей ред. В.В. Блажеева, М.А. Егоровой. М., 2022.

23. Мажорина М.В. ESG-принципы в международном бизнесе и «устойчивые контракты» // Актуальные проблемы российского права. 2021. Т.

16. № 12(133). Декабрь.

24. Петрова Д.А. Правовые режимы защиты персональных данных в условиях цифровизации // Advances in Law Studies. 2020. Том 8. № 5.

25. Правовое регулирование искусственного интеллекта в условиях пандемии и инфодемии: монография / под общей ред. В.В. Блажеева, М.А. Егоровой. М.: Проспект, 2020.

Интернет-источники:

26. ESG-повестка как новый тренд российского бизнеса. URL: http://rapsinews.ru/incident_publication/20220321/307803134.html (дата обращения: 10.10.2022).

27. KPMG. Время устойчивых: почему бизнес больше не может игнорировать ESG-повестку? URL: https://mustread.kpmg.ru/articles/vremya-ustoychivykh-pochemu-biznes-bolshe-ne-mozhet-ignorirovat-esg-povestku/ (дата обращения: 10.10.2022).

28. Отчет 1 НИУ ВШЭ. URL: https://old.sk.ru/foundation/legal/p/03.aspx (дата обращения: 10.09.2022).

29. Сбер выпустил первый обзор ESG-трендов в России. URL: https://press.sber.ru/publications/sber-vypustil-pervyi-obzor-esg-trendov-v-rossii (дата обращения: 08.10.2022).

30. Are Privacy and Cybersecurity the Next Frontier for ESG? URL: https://www.treasuryandrisk.com/2022/02/10/is-privacy-and-cybersecurity-the-next-frontier-for-esg-411-26421/ (дата обращения: 10.10.2022).

31. Blackstone. An Integrated Approach to ESG. URL: https://www.blackstone.com/wp-content/uploads/sites/2/2021/11/2021-ESG-Update_An-Integrated-Approach-to-ESG.pdf (дата обращения: 10.10.2022).

32. BlackRock Takes Sustainable Investing Mainstream with Range of Low-Cost Sustainable Core ETFs. URL: https://ir.blackrock.com/news-and-events/press-releases/press-releases-details/2018/BlackRock-Takes-Sustainable-Investing-

Mainstream-with-Range-of-Low-Cost-Sustainable-Core-ETFs/default.aspx (дата обращения: 08.10.2022).

33. Connect privacy with ESG to drive broader business success. URL: https://www.ey.com/en_ca/sustainability/connect-privacy-with-esg-to-drive-broader-business-success (дата обращения: 01.10.2022).

34. Data Governance, Privacy and Trust – A Sweet Spot for ESG? URL: https://www.herbertsmithfreehills.com/insight/data-governance-privacy-and-trust-–-a-sweet-spot-for-esg (дата обращения: 10.10.2022).

35. Data Privacy & ESG. URL: https://redcloveradvisors.com/2021/05/21/data-privacy-esg-2/ (дата обращения: 05.10.2022).

36. Data Protection as a Corporate Social Responsibility. From Compliance to Sustainability to Generate Both Social and Financial Value. URL: https://www.maastrichtuniversity.nl/data-protection-corporate-social-responsibility (дата обращения: 10.10.2022).

37. Dentsu. White Paper. Устойчивое развитие & ESG. Гайд для маркетологов 2022. URL: https://assets-eu-01.kc-usercontent.com/296d8d4d-1c46-01bf-48d9-7c150d2fc3b5/c7d00561-f02b-4734-acd5-1b88ce215893/Dentsu%20S ustainability%20&%20ESG_2022.pdf (дата обращения: 09.10.2022).

38. DLI PIPER. Data Protection Laws of the World – Canada. URL: https://www.dlapiperdataprotection.com/index.html?t=definitions&c=CA&c2= (дата обращения: 20.09.2022).

39. DLI PIPER. Data Protection Laws of the World – Japan. URL: https://www.dlapiperdataprotection.com/index.html?t=definitions&c=JP&c2= (дата обращения: 20.09.2022).

40. DLI PIPER. Data Protection Laws of the World – United Kingdom. URL: https://www.dlapiperdataprotection.com/index.html?t=law&c=GB (дата обращения: 20.09.2022).

41. DLI PIPER. Data Protection Laws of the World – Singapore. URL: https://www.dlapiperdataprotection.com/index.html?t=definitions&c=SG&c2= (дата обращения: 20.09.2022).

42. Edelman`s 2018 Earned Brand Study. October 2, 2018. URL: https://www.edelman.com/earned-brand (дата обращения: 08.10.2022).

43. ESG and Privacy – a Foundation for Better Compliance? URL: https://www.alvarezandmarsal.com/insights/esg-and-privacy-foundation-better-compliance (дата обращения: 10.10.2022).

44. ESG as the Next Frontier in Privacy and Data Governance: Moving Beyond Regulatory Compliance. URL: https://www.treasuryandrisk.com/2022/02/10/is-privacy-and-cybersecurity-the-next-frontier-for-esg-411-26421/c6b692ff-e718-4b36-a5f5-059ead10d552 (дата обращения: 10.10.2022).

45. ESG Data Privacy and Protection. URL: https://www.alpha-sense.com/blog/data-privacy-esg/ (дата обращения: 01.10.2022).

46. Facebook data privacy issue already identified by ESG investment screens. URL: https://www.investmentnews.com/facebook-data-privacy-issue-already-identified-by-esg-investment-screens-75033 (дата обращения: 10.10.2022).

47. IDC: Expect 175 zettabytes of data worldwide by 2025. URL: https://www.networkworld.com/article/3325397/idc-expect-175-zettabytes-of-data-worldwide-by-2025.html (дата обращения: 08.10.2022).

48. Privacy, Data Protection is Top ESG Concern Among Consumers. URL: https://blog.451alliance.com/privacy-data-protection-is-top-esg-concern-among-consumers/ (дата обращения: 08.10.2022).

49. Singapore – Data Protection Overview. URL: https://www.dataguidance.com/notes/singapore-data-protection-overview (дата обращения: 20.09.2022).

50. Socially responsible investors reassess Facebook ownership. URL: https://www.reuters.com/article/us-facebook-cambridge-analytica-funds-an-idUSKBN1GV318 (дата обращения: 05.10.2022).

51. The climate impact of ICT: A review of estimates, trends and regulations. URL: https://arxiv.org/ftp/arxiv/papers/2102/2102.02622.pdf (дата обращения: 09.10.2022).

52. The EU General Data Protection Regulation. Questions and Answers. URL: https://www.hrw.org/news/2018/06/06/eu-general-data-protection-regulation (дата обращения: 09.10.2022).

53. The Role of Data Privacy and Security in ESG (Environmental, Social, Governance) https://www.ardentprivacy.ai/the-role-of-data-privacy-and-security-in-esg-environmental-social-governance/ (дата обращения: 08.10.2022).

54. Your ESG fund might be invested in Facebook – and it highlights a major issue with sustainable investing. URL: https://www.cnbc.com/2021/10/26/your-esg-fund-might-be-invested-in-facebook.html (дата обращения: 05.10.2022).

55. Your ESGuide in 5: Finding the P for Privacy in ESG. URL: https://www.lexology.com/library/detail.aspx?g=8b1a2950-a343-4822-a751-06f19089cbf4 (дата обращения: 10.10.2022).

56. Verizon. Digital responsibility. Privacy and data protection. URL: https://www.verizon.com/about/sites/default/files/esg-report/2019/social/digital-responsibility/privacy-and-data-protection.html (дата обращения: 10.10.2022).

57. Verizon Will Pay $350 Million +Less for Yahoo. URL: https://www.nytimes.com/2017/02/21/technology/verizon-will-pay-350-million-less-for-yahoo.html (дата обращения: 03.10.2022).

58. What is personal data? URL: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en (дата обращения: 20.09.2022).

59. Why Data Privacy Is an ESG Issue. URL: https://www.theimpactivate.com/why-data-privacy-is-an-esg-issue/ (дата обращения: 01.10.2022).

60. Why is Cybersecurity Important to ESG Frameworks? URL:

https://www.jpmorgan.com/insights/research/why-is-cybersecurity-important-to-esg (дата обращения: 09.10.2022).

61. 1 in 4 investing dollars are now going into ESG strategies. How to play it, according to Cowen. URL: https://www.cnbc.com/2021/03/18/sustainable-strategies-attract-1-in-4-investing-dollars.html (дата обращения: 10.10.2022).