https://www.oecd.org/science/oslo-manual-2018-9789264304604-en.html (date of access: 18.12.2024).

8. Mazzi A. Introduction. Life cycle thinking / ed. Jingzheng Ren, Sara Toniolo, Life Cycle Sustainability Assessment for Decision-Making, Elsevier. 2020. P. 1–19. URL: https://doi.org/10.1016/B978-0-12- 818355-7.00001-4 (date of accessed: 15.09.2023).

9. PropTech 3.0: The Future of Real Estate. URL: https://www.sbs.oxford.edu (date of accessed: 10.02.2025).

10. Saat, Z. M. Assessment of property management service quality of purpose built office buildings [Electronic resource] / Z. M. Saat, A. H. Nawawi, Z. A. Baharum // Intern. Business Research. – 2009. – Vol. 2, № 1. – Mode of access: https://pdfs.semanticscholar.org/229a/df4a8c5473a8274ce7951ab94169bd62dd47.pdf. – Date of access: 20.12.2024.

УДК 338.2-027.45(476)

В.Б. Криштаносов
зав. кафедрой ЭТиМ, канд. экон. наук
(БГТУ, г. Минск)

РИСКИ И УГРОЗЫ УТЕЧКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ КАК ФАКТОР СНИЖЕНИЯ ДОВЕРИЯ НАСЕЛЕНИЯ К ГОСУДАРСТВЕННЫМ ИНСТИТУТАМ

Цифровые услуги, предоставляемые государственными организациями, в современном мире становятся лицом государства. Если качество предоставляемых услуг высокое, обеспечивается надлежащая защита персональных данных граждан, это укрепляет доверие общества к государственным институтам. Следует отметить, что цифровые данные, агрегируемые государственными организациями, обладают значительной ценностью и могут быть классифицированы на:

1. Данные, которые относятся к категории «государственная тайна» (военные и разведывательные секреты, сведения об экономической политике государства, информация о внешнеполитической деятельности и т.д.). Нарушение секретной информации может поставить под угрозу национальную безопасность, раскрыть военные стратегии и выявить уязвимости для противников.

2. Финансовые отчеты включают информацию о налогоплательщиках, государственные бюджеты, экономические отчеты и записи транзакций, которые необходимы для управления государственными средствами и для обеспечения стабильной деятельности государ-

ства. Нарушение конфиденциальности и целостности данных может привести к мошенническим действиям, таким как кража средств или манипулирование финансовыми отчетами. Более того, раскрытие этой информации может ослабить доверие общества к государственным учреждениям и привести к значительным финансовым потерям.

3. В категорию «персональные данные граждан», согласно Закону Республики Беларусь «О защите персональных данных» № 99-З от 7 мая 2021 г., включается любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано. Отдельно необходимо отметить биометрические данные, которые используются не только в качестве метода авторизации, но и инструмента осуществления оплаты.

Если в отношении информации, классифицированной как «государственная тайна», финансовой отчетности, государственными органами управления наработана практика обеспечения необходимой безопасности, то оцифрованные *персональные данные граждан* являются новым объектом регулирования. Обеспечение их ненадлежащей безопасности может привести к негативным последствиям, позволяя киберпреступникам оказывать давление, получать стратегические преимущества и достигать своих политических и военных целей. Именно угроза критической инфраструктуре и кража конфиденциальной информации формирует условия для дестабилизации органов государственного управления, подрыва общественное доверие и манипулирования международными отношениями. В последние годы распространилась практика проведения кибератак, спонсируемых недружественными государствами. В отчете Microsoft Digital Defense за 2022 год отмечен двукратный рост количества кибератак со стороны правительств, направленных на критически важную инфраструктуру, – с 20% до 40% [1].

Таким образом, *государственные системы* являются привлекательной мишенью для киберпреступников. Так, по данным Агентства Европейского Союза по кибербезопасности за 2023 год государственный сектор возглавил список целевых областей кибератак, на долю которого пришлось 24% зарегистрированных случаев. По данным Kaspersky Security Network, в 2024 году правительственные ресурсы заняли третье место среди сфер, атакованных киберпреступниками, на ее долю пришлось 14% всех зарегистрированных атак. Кроме того, в 2024 году также значительно увеличилось число *утечек данных*. Так, ресурсный центр по борьбе с кражей персональных данных (ITRC) сообщил о 1571 крупном случае компрометации данных, затронувших около 1,07 млрд. человек. Число жертв утечек данных увеличилось на

490 % по сравнению с 2023 годом [2]. При этом наибольшее число утечек конфиденциальной информации по итогам первого полугодия 2024 г. приходилось именно на госучреждения – 13% (см. рис. 1).

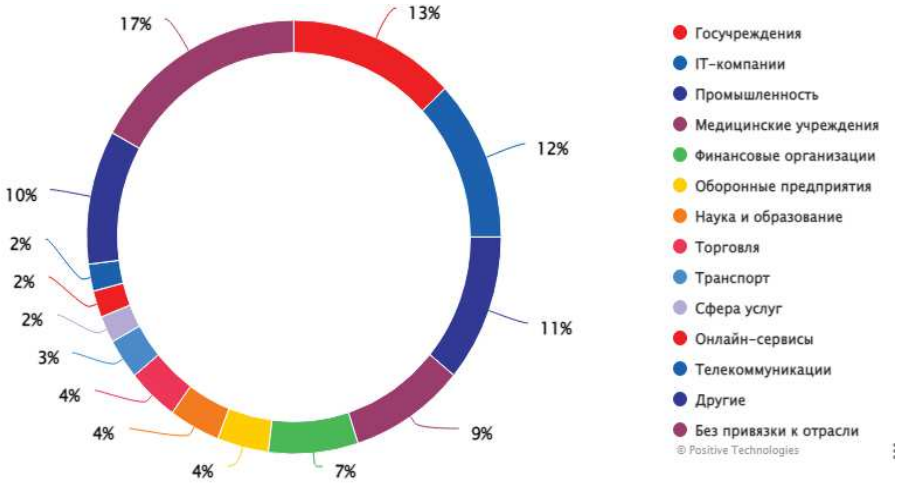

Рисунок 1 – Распределение количества утечек по отраслям

В Республике Беларусь в 2023 году несанкционированно в Сеть утекли данные около 1 млн граждан страны. Это данные клиентов интернет-магазина «Остров чистоты и вкуса» (730 тыс.), интернет-магазина «Буслік» (220 тыс.), предприятия по производству дверей «Юркас» (5 тыс.) [3]. При этом абсолютное большинство утечек было связано с уязвимостью систем «Битрикс». В 2024 году Национальный центр защиты персональных данных получил 6 уведомлений о нарушениях системы защиты персональных данных, утечки коснулись около 2 млн записей с данными белорусских граждан. По информации центра, на торговлю и остальную сферу услуг приходится более 95% от общего объема персональных данных, которые незаконным образом были распространены в Сети.

Среди *особенностей организаций государственного сектора*, связанных с обеспечением цифровой безопасности, следует выделить: жесткие бюджетные ограничения, которые не позволяют предложить ИТ специалистам конкурентоспособную на рынке заработную плату, обеспечить найм достаточного количества сотрудников по кибербезопасности, обновить устаревшие системы и ИКТ инфраструктуру, уязвимую для кибератак. Многие государственные организации полагаются на запатентованные системы, несовместимые с новейшими технологиями, что ограничивает их способность обеспечивать цифровую безопасность. Усложняет ситуацию, тот факт, что государственные организации должны балансировать между поддержанием устаревших систем и модернизацией своей инфраструктуры для удовлетворения современных требований кибербезопасности. Кроме того,

важно отметить, что риски цифровой безопасности не ограничиваются непосредственно государственными организациями - они распространяются на сторонних поставщиков и подрядчиков, которые с ними взаимодействуют.

1. Основные риски и угрозы.

Важно классифицировать утечки персональных данных на два типа: *неумышленные*: возникают под действием факторов среды, форс-мажорных обстоятельств; умышленные, спровоцированные определенными людьми, их действиями с конкретной целью. Так, проведенное в 2021 российской компанией Солар исследование «Случайные утечки информации в госорганах», показало, что свыше 90% руководителей госпредприятий видят наибольшую угрозу именно в случайных инцидентах, нежели в подготовленных заранее сливах конфиденциальных сведений. Однако, на практике доля умышленных случаев информационных утечек составляет 36,2%, в то время как самопроизвольно произошедших – всего 12,8%. Спровоцировать случайную утечку информации могут отсутствие или поверхностные знания в области информационной безопасности – свыше 55% респондентов, перегруженность сотрудников госорганов многочисленными задачами – свыше 30% респондентов. Свыше 10% респондентов считают, что провоцируют случайные утечки информации в госорганах невнимательность, обеспечивающая пресловутый человеческий фактор.

Вместе с тем утечки правительственных данных часто являются результатом действий отдельных лиц или групп, стремящихся использовать конфиденциальную информацию, хранящуюся в государственных учреждениях. Эти нарушения могут привести к краже, раскрытию или неправомерному использованию персональных данных, создавая угрозу национальной безопасности, нарушая работу государственных служб и ставя под угрозу конфиденциальность граждан. По данным российской группы компаний InfoWatch, в России в 2024 году более 80% утечек информации произошло в результате кибератак [4]. Наибольшее количество инцидентов зафиксировано в розничной торговле, включая онлайн- и офлайн-сегменты. В 2024 году на нее пришлось 27,8% всех утечек и 35,1% случаев компрометации персональных данных. На втором месте – государственные учреждения (18% от всех утечек). При этом следует отметить, что компрометация учетных данных, как правило, не является конечной целью киберпреступников и служит промежуточным этапом между проникновением в атакуемую инфраструктуру и развитием атаки до наступления иных послед-

ствий – например, нарушения работоспособности системы, кражи денежных средств или иной конфиденциальной информации.

Традиционно *основными методами кибератак*, которые привели к утечке конфиденциальной информации в первом полугодии 2024 г., стали использование злоумышленниками вредоносного ПО, социальная инженерия и эксплуатация уязвимостей (см. рис. 2).

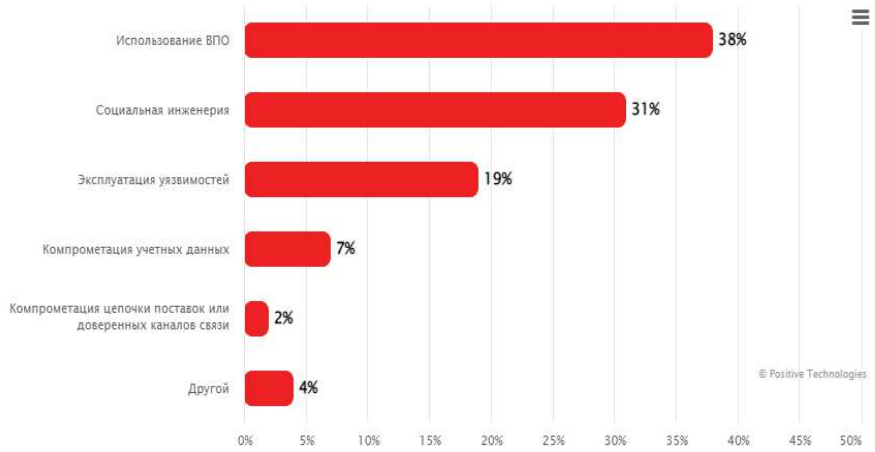

Рисунок 2 – Методы, использованные в успешных атаках на организации, последствием которых стала утечка

2. Последствия утечки персональных данных для доверия населения к государственным органам власти.

Следует выделить следующие *последствия кибератак*, направленных на кражу персональных данных:

– *утрата конфиденциальности*: по данным опроса, опубликованного в 2023 году Управлением австралийского комиссара по информации (OAIC), $^{3}/_{4}$ опрошенных граждан страны считают, что утечка данных является самым большим риском для конфиденциальности, с которым они сталкиваются. Более того, 70% австралийцев придают большое значение конфиденциальности при выборе того или иного продукта или услуги: после качества и цены продукта именно конфиденциальность данных является третьим по важности фактором.

– *репутационный ущерб*: эрозия статуса и репутации организации в глазах населения. Как показали исследования компании IBM о стоимости утечки данных в 2023 году, до 30% пользователей перестанут вести дела с организациями, которые подверглись взлому. Кроме того, 85% расскажут другим о своем опыте, а 33,5% воспользуются социальными сетями, чтобы выразить свое недовольство. В США, как выявило исследование американской компании Vercara в 2024 году, 66% пользователей перестают доверять организации, ставшей жертвой утечки данных, а 44% пользователей связывают киберинциденты с отсутствием у нее мер надлежащей цифровой безопасности [5].

Центр компетенций группы компаний Гарда выяснил, что в 2024 году 69% россиян заявили, что не будут пользоваться услугами организации, допустившей утечку персональных данных.

− *финансовые издержки* выражаются в прямом денежном и вероятном ущербе из-за потери целостности и конфиденциальности цифровых данных. Кибератака приводит к прямым затратам, таким как выплаты выкупа, расходы на восстановление системы и судебные издержки, а также к косвенным затратам, таким как потеря общественного доверия и ущерб репутации. Например, атака программы-вымогателя WannaCry в 2017 году привела к финансовым потерям на сумму около 4 млрд. долларов во всем мире, нарушив работу критически важных служб и потребовав значительных ресурсов для восстановления инфраструктуры. Взлом Управления кадров США (OPM) в 2015 году привел к расходам примерно в 600 млн долларов, связанным с услугами кредитного мониторинга, защитой от кражи личных данных и модернизацией систем цифровой безопасности. Взлом SolarWinds в 2020 году обошелся пострадавшим организациям, включая государственные учреждения, в более чем 100 млн долларов США на реагирование на инциденты и устранение последствий кибератаки.

− *перебои в операционной деятельности*: взлом киберпреступниками цифровых систем местных органов власти, полицейских управлений или служб здравоохранения, может привести к перебоям в обслуживании, утечке секретных данных, повреждению критической инфраструктуры, угрозе жизни и здоровью граждан. Так, кибератака программы-вымогателя Wannacry на Национальную службу здравоохранения (NHS) Великобритании затронула более 600 организаций, которые были лишены доступа к своим цифровым системам и медицинским устройствам. В результате были отменены около 19 тыс. посещений врача, включая критически важные хирургические операции.

− *снижение участия граждан в цифровых сервисах*: опасение утечек снижает мотивацию населения к использованию электронных госуслуг. Генерирование СМИ информационных потоков о массовых нарушениях кибербезопасности приводит к созданию «фактора страха» граждан в отношении безопасности собственной цифровой деятельности, даже если нарушение не затронуло их напрямую. Это может привести к сокращению онлайн-активности, нежеланию внедрять новые технологии и даже к возврату к менее удобным, нецифровым альтернативам.

− *политический скептицизм*: население начинает сомневаться в компетентности власти в отношении возможности обеспечить в стране цифровую безопасность, что в определенных условиях может

спровоцировать социальный протест. Например, в 2024 году во время выборов в Индии произошла утечка базы данных, содержащей отпечатки пальцев и сканы лиц полицейских, военнослужащих и гражданских лиц, что вызвало опасения по поводу кражи личных данных и безопасности выборов. Взлом в 2015 году Управления кадров США (OPM), в результате которого были раскрыты личные данные 21,5 миллиона федеральных служащих, вызвал широкое общественное возмущение[1].

К *факторам усиления кризиса доверия граждан* к государственным органам власти следует также отнести:

− недостаточную прозрачность государственных организаций, сокрытие инцидентов или задержки в информировании граждан;

− отсутствие надлежащей отчётности, нежелание наказывать виновных или проводить модернизацию системы после утечек;

− пробелы в законодательстве: несоответствие мер защиты организации национальным или международным стандартам.

3. *Среди наиболее крупных инцидентов*, связанных с утечкой персональных данных, следует выделить кибератаку в 2024 году на ведущего поставщика технологий в сфере медицинского страхования Change Healthcare (*США*), которая привела к сбоям в работе здравоохранения по всей стране и утечке персональных данных. В результате атаки были раскрыты конфиденциальные медицинские данные пациентов (диагнозы, лекарства, результаты тестов, изображения, показания к уходу и лечению). Масштабная кибератакана компанию NRS Healthcare (*Великобритания*) привела к утечке персональных данных, а также более 600 тыс. документов, в том числе контрактов и финансовых отчетов. Имела место утечка персональных данных более 5 млн граждан *Сальвадора*, что составляет около 80% от всего населения страны. Атака на муниципалитет Дубая (*ОАЭ*) привела к краже удостоверений личности, паспортов и других файлов с персональными данными граждан страны. Правительственное агентство France Travail (*Франция*), ответственное за регистрацию безработных, в результате кибератаки столкнулось с утечкой персональных данных 43 млн граждан (что составляет 60% от всего населения). В *Индии* утечка персональных данных из телекоммуникационных компаний затронула около половины граждан страны (750 млн человек).

[1]Вместе с тем, результаты исследования, проведенного в 2023 году Ш.Матциным, Р.Шандлером, Д.Канетти и опубликованного в издании «TheBritishJournalofPoliticsandInternationalRelations», показали на примере опроса около 2 тыс. респондентов из США, Великобритании и Израиля, чтокибератаки на критически важную инфраструктуру не подрывают доверие к правительству. Более того, негативные эмоции – в первую очередь гнев – играют решающую роль в повышении доверия к правительству в Соединенных Штатах (но не в Великобритании или Израиле).

В 2023 году из Единого госреестра недвижимости *России* произошла утечка персональных данных нескольких миллионов граждан страны. Кибератака на систему здравоохранения *Ирландии* в 2021 году, привела к масштабному отказу в медицинских услугах и общественному недовольству.

В период с 2020 по 2023 гг. в *Таиланде* произошло как минимум три крупных кражи персональных данных. Так, в 2021 году персональные данные примерно 106 млн резидентов и нерезидентов страны стали доступны онлайн. В 2023 году выставлены на продажу в даркнете личные данные 55 млн граждан, полученные в результате взлома с таиландского национального портала общественного здравоохранения, а также персональная информация 20 млн граждан, украденных из правительственных учреждений (главным образом из Департамента по делам пожилых людей).

В результате взлома ИТ компании SolarWinds (*США*) в 2020 году киберпреступники проникли в несколько правительственных учреждений США посредством скомпрометированных обновлений программного обеспечения. В результате этого нарушения были раскрыты конфиденциальные данные федеральных агентств. Одна из самых значительных утечек данных в истории произошла в одном из крупнейших агентств кредитной отчетности Equifax (*США*) в 2017 году: отмечена кража персональных данных 147 млн человек. Это привело к широкому общественному возмущению, множеству судебных исков и мировому соглашению на сумму до 700 млн долларов. Результатом инцидента стало резкое падение доверия потребителей к агентствам кредитной отчетности и финансовым учреждениям страны в целом.

4. Механизмы минимизации рисков.

а) приоритезация цифровой безопасности в рамках отдельных организаций и в стране в целом. Осуществление данной политики предполагает донесение до граждан, от ИТ-специалистов до рядовых сотрудников, важности кибербезопасности. Требуется регулярное обучение по таким темам, как предотвращение фишинга, безопасное управление паролями и безопасный просмотр контента в сети Интернет.

б) важным механизмом обеспечения цифровой безопасности в целом и предотвращения утечки персональных данных в частности является развитие сотрудничества между государственными организациями и частным сектором. Обмен информацией об угрозах, передовым опытом и извлеченными уроками укрепляет защиту и помогает более эффективно реагировать на новые угрозы.

в) регулярное тестирование и оценка уязвимостей. Данное направление включает в себя тестирование на проникновение, имитирующее кибератаки для выявления уязвимостей системы, и постоянное сканирование уязвимостей для проверки наличия потенциальных пробелов в безопасности. Данные стратегии защищают конфиденциальность, целостность и доступность персональных данных, содержащихся в государственных органах власти, имеющих решающее значение для бесперебойного функционирования государственных служб и безопасности граждан.

г) с ростом киберугроз, нацеленных на правительственные системы, ключевую роль в минимизации рисков играют превентивные меры, такие как надежное *шифрование*. Преобразование данных в нечитаемые форматы с помощью алгоритмов шифрования позволяет обеспечить доступ к информации только для авторизованных пользователей с ключом расшифровки. Государственным организациям следует внедрить передовые стандарты шифрования (AES) для защиты данных как при хранении, так и при передаче, обеспечивая безопасность даже в случае перехвата. Регулярные проверки систем хранения данных необходимы для выявления и устранения потенциальных уязвимостей, которыми могут воспользоваться киберпреступники. Более того, шифрование должно быть интегрировано на все этапы обработки данных, включая передачу, хранение и резервное копирование, чтобы обеспечить комплексную безопасность.

В Республике Беларусь техническая и криптографическая защита персональных данных осуществляется в порядке, установленном Оперативно-аналитическим центром при Президенте Республики Беларусь, в соответствии с классификацией информационных ресурсов (систем), содержащих персональные данные.

д) строгий контроль доступа: Многофакторная аутентификация (MFA) и модели нулевого доверия (Zero Trust). MFA требует от пользователей предоставления двух или более форм идентификации для доступа к системам, добавляя дополнительный уровень безопасности. Такой подход существенно затрудняет доступ неавторизованных лиц, даже если они получили учетные данные для входа. Внедрение архитектуры Zero Trust еще больше усиливает безопасность, поскольку предполагается, что ни один пользователь или устройство не пользуется доверием по своей сути, даже если они находятся в сети. Эта модель требует постоянной проверки на каждом этапе доступа, обеспечивая постоянное поддержание безопасности.

е) инструменты мониторинга в реальном времени, такие как системы обнаружения вторжений (IDS), играют решающую роль в выявлении угроз и реагировании на них по мере их возникновения.

Эти системы постоянно анализируют сетевой трафик на наличие признаков подозрительной активности, позволяя организациям обнаруживать потенциальные нарушения.

ж) важным элементом защиты от случайных и умышленных утечек конфиденциальной информации выступают DLP-системы, которые отслеживают и блокируют попытки передачи информации вне пределов корпоративной сети.

з) использование *соглашений о неразглашении коммерческой тайны (NDA),* в которых закрепляется ответственность работников за нарушение данного договора.

и) введение адекватного размера *штрафов* за ненадлежащую работу организаций с персональными данными граждан. Например, в соответствии с европейским стандартом по защите данных GDPR и стандартом Великобритании UK Data Protection Act штраф может составить до 4% от годового оборота компании или 20 миллионов евро, в зависимости от того, что больше. Законодательство в Сингапуре и Австралии предусматривает штрафы до 10% от годового оборота, а в Бразилии – 2%. В 2023 году Ирландская комиссия по защите данных (DPC) наложила исторический штраф в размере 1,2 миллиарда евро на американского технологического гиганта Meta. В России в 2024 году принят закон, повышающий ответственность за компрометацию персональных данных для утечки, затрагивающей более 100 тыс. человек или свыше 1 млн. записей персональных данных: для физических лиц размер штрафа на сумму до 400 тыс. росс. рублей, должностные лица – до 600 тыс. росс. рублей, юридические лица – на сумму до 15 млн росс. рублей.

В Республике Беларусь несоблюдение мер обеспечения защиты персональных данных физических лиц влечет наложение штрафа в размере от 2 до 10 базовых величин, на индивидуального предпринимателя – от 10 до 25 базовых величин, а на юридическое лицо – от 20 до 50 базовых величин.

Утечки правительственных данных представляют собой серьезную угрозу национальной безопасности и общественному доверию. Чтобы минимизировать эти риски, крайне важно внедрить надежные системы кибербезопасности, надежное шифрование и системы упреждающего мониторинга. Государство должно сделать кибербезопасность постоянным приоритетом и постоянно совершенствовать защиту персональных данных.

Утечки персональных данных не только угрожают приватности граждан, но и становятся катализатором системного кризиса доверия к государству. Для предотвращения этого необходима комбинация тех-

нологических, правовых и коммуникационных мер, а также открытый диалог между властью и обществом. Без этого цифровая трансформация госуслуг может привести к обратному эффекту – росту социальной напряжённости.

ЛИТЕРАТУРА

1. Digital Defense Report // Microsoft. – 2022. – 114 p. – URL: https://go.microsoft.com/fwlink/?linkid=2213817&clcid=0x413&culture=nl-nl&country=nl (date of access: 02.03.2023).

2. H1 2024 Data Breach Analysis // The Identity Theft Resource Center (ITRC). – 2024. – URL: https://www.idtheftcenter.org/publications (date of access: 12.05.2025).

3. Ветрова А. В Беларуси в сеть утекли данные более миллиона человек: кто виноват и что делать, чем утечка грозит потребителю, как дать согласие на обработку своих данных и как его забрать // Belarus.kp.ru. – 2023. – URL: https://www.belarus.kp.ru/daily/27527/4791726/ (дата обращения: 10.01.2024).

4. Эксперты зафиксировали снижение утечек из российских финансовых компаний // expert.ru. – 2025. – URL: https://expert.ru/news/eksperty-zafiksirovali-snizhenie-utechek-iz-rossiyskikh-finansovykh-kompaniy/ (дата обращения: 12.05.2025).

5. New Vercara Research Reveals Impact of Trust in Brands Following Breaches, Concerns Around Outside Threats // vercara.digicert.com. – 2024. – URL: https://vercara.digicert.com/news/new-vercara-research-reveals-impact-of-trust-in-brands-following-breaches-concerns-around-outside-threats (date of access: 12.05.2025).

УДК 620.95:662.638

А.В. Ледницкий, доц., канд. экон. наук;
П.А. Протас, доц., канд. техн. наук;
Ю.И. Мисуно, ассист.;
Л.Ю. Пшебельская, доц., канд. экон. наук (БГТУ, г. Минск)

ВОЗОБНОВЛЯЕМЫЕ ИСТОЧНИКИ ЭНЕРГИИ КАК ДРАЙВЕР ЗЕЛЁНОЙ ЭКОНОМИКИ РЕСПУБЛИКИ БЕЛАРУСЬ

Повестка дня в области устойчивого развития на период до 2030 года, принятая 25 сентября 2015 года 193 странами мира, свидетельствует о том, что дальнейшее экономическое развитие стран возможно лишь на основе совместных усилий правительств, частного сектора и гражданского общества по достижению 17 целей устойчивого разви-