Наконечная Ульяна Владимировна
студентка
Научный руководитель
Фомичева Татьяна Леонидовна
канд. экон. наук, доцент
ФГОБУ ВО «Финансовый университет
при Правительстве Российской Федерации»
г. Москва

ПРОБЛЕМЫ ЗАЩИТЫ ПОЛЬЗОВАТЕЛЬСКИХ ДАННЫХ В БИЗНЕС-ЭКОСИСТЕМАХ

Аннотация: *в статье исследуется, как организации в контексте бизнес-экосистемы меняют требования к защите пользовательских данных. Особое внимание уделяется теоретическим аспектам безопасности бизнес-экосистем, анализу возникающих угроз и инструментам их решения, включая законодательные требования.*

Ключевые слова: *бизнес-экосистема, защита данных, персональные данные, информационная безопасность, утечки данных, цифровые платформы.*

Современный бизнес всё чаще строится как экосистема. Компании объединяются вокруг одной платформы. В контексте безопасности данных экосистема создаёт общую среду, в которой пользовательские данные перестают принадлежать одному сервису.

Теоретические представления бизнес-экосистем в проблемах защиты данных.

Развитие цифровых бизнес-экосистем сопровождается увеличением объёмов обрабатываемой информации и расширением взаимодействия между участниками. В связи с этим защита пользовательских данных становится одним из ключевых условий устойчивого.

К основным признакам цифровых бизнес-экосистем относят модульность, сетевой эффект и централизованную идентификацию [1]. Каждый из них создаёт

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

риски для информационной безопасности. Модульность увеличивает количество подключённых сервисов и каналов обмена данными, сетевой эффект усиливает число потенциальных уязвимостей, а централизованная идентификация создаёт единую точку риска. Взлом одной учётной записи может открыть доступ к информации нескольких сервисов. В отличие от отдельной цифровой платформы, бизнес-экосистема объединяет несколько взаимосвязанных участников, поэтому нарушение безопасности одного из них может затронуть не только собственных клиентов, но и пользователей других сервисов. Это усложняет контроль за движением данных и распределением ответственности между участниками.

С экономической точки зрения проблема защиты данных связана с распределением затрат и ответственности. Р. Андерсон и Т. Мур отмечают, что последствия недостаточной защиты информации затрагивают компании и пользователей [3]. Модель Л. Гордона и М. Лоеба предполагает соотнесение расходов на информационную безопасность с ожидаемыми потерями и приоритетную защиту наиболее ценных и уязвимых данных [6]. Поэтому цифровая экосистема должна учитывать безопасность всей системы.

Кроме того, ещё одной проблемой является получение согласия пользователя на обработку персональных данных. Как отмечает Я. А. Карунная со ссылкой на Н. А. Ястреба, отсутствие специальных знаний затрудняет понимание человеком того, на какую обработку информации он соглашается [5]. При этом отказ от согласия ограничивает доступ к услуге. В цифровых бизнес-экосистемах проблема усугубляется, потому что данные пользователя могут использоваться сразу несколькими взаимосвязанными сервисами.

Практические проявления и инструменты защиты данных.

Проявление рисков защиты пользовательских данных заметны на практике. К примеру, в марте 2022 года произошла масштабная утечка данных пользователей сервиса «Яндекс Еда», в результате которой в открытый доступ попало около 49 млн строк с информацией о клиентах. Этот случай показал, что утечка в рамках одного цифрового сервиса может затронуть значительное количество пользователей и негативно повлиять на доверие к связанным с ним цифровым услугам.

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

Масштаб проблемы подтверждается общероссийской статистикой. По данным Роскомнадзора, в 2024 году было зафиксировано 135 случаев утечки персональных данных, в результате которых в открытый доступ попало более 710 млн записей. В 2025 году количество выявленных инцидентов снизилось до 118, а объём утекших данных составил более 52 млн записей. Несмотря на снижение показателей, масштабы утечек остаются значительными, что свидетельствует о сохраняющейся актуальности проблемы защиты персональных данных [7].

Среди основных причин утечек А. С. Селюк выделяет социальную инженерию, прежде всего фишинг, недостаточную защиту учётных записей, уязвимости при обработке информации с использованием искусственного интеллекта и неправомерные действия сотрудников [4]. Последствия подобных инцидентов отражаются на доверии потребителей. Согласно исследованию В. Н. Довжика с соавторами, 79% представителей поколения X не доверяют единой авторизации через экосистемные аккаунты [1]. Обеспечение информационной безопасности становится экономической задачей, влияющей на репутацию компаний и доверие пользователей.

Инструменты защиты данных.

Инструменты защиты можно разделить на правовые и организационно-технические.

К правовым относится прежде всего Федеральный закон №152-ФЗ «О персональных данных». Закон устанавливает требования к законности обработки персональных данных, в том числе получению согласия пользователя в предусмотренных случаях. При сборе персональных данных граждан РФ их первичная запись, систематизация, накопление, хранение, уточнение и извлечение должны осуществляться с использованием баз данных, находящихся на территории России, за исключением установленных законом случаев. С сентября 2022 года коммерческие и государственные организации обязаны сообщать уполномоченному органу об утечке данных и о результатах внутренней проверки [8]. После принятия Федерального закона №420-ФЗ, вступившего в силу 30 мая 2025 года, ответ-

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

ственность компаний за утечки персональных данных значительно ужесточилась. За первую утечку юридическому лицу грозит штраф от 3 до 15 млн рублей. Если компания допускает повторную крупную утечку, штраф рассчитывается исходя из её годовой выручки [9].

Организационно-технические меры.

1. Минимизация данных. Каждый сервис получает только те сведения, которые нужны ему для работы.

2. Модель «нулевого доверия». Каждый запрос на доступ проверяется независимо откуда он пришёл.

3. Шифрование и обезличивание. Такие данные теряют часть ценности для злоумышленника, но остаются пригодными для аналитики.

4. Контроль партнёров. Единые требования к безопасности, регулярные проверки, ограничение прав доступа и возможность быстро отключить участника при инциденте.

5. Внутренние стандарты и обучение сотрудников. По оценке А. С. Селюка, именно внутренние механизмы защиты должны стоять на первом месте [4].

Тенденции развития защиты данных в бизнес-экосистемах.

Развитие защиты данных в бизнес-экосистемах связано с ростом киберугроз и ужесточением государственного регулирования. В ближайшие годы можно выделить несколько основных тенденций.

Совершенствование_законодательства. Д. А. Рыжков отмечает необходимость заранее формировать правовую базу для регулирования экосистем, учитывая опыт стран, в которых они получили широкое распространение [2].

Ужесточение_ответственности_бизнеса. Рост штрафов за утечки данных будет стимулировать компании уделять больше внимания информационной безопасности и увеличивать расходы на её обеспечение.

Расширение_использования_ИИ_и_биометрии. Применение персональных данных для обучения алгоритмов и распознавания лиц создаёт новые угрозы. Поэтому особое значение приобретает информирование пользователей о том, как используются их данные.

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

Развитие_отечественных_технологий. Недостаток российских программных решений в сфере информационной безопасности, на который обращает внимание А. С. Селюк, будет способствовать росту спроса на отечественные разработки [4]

Усиление_контроля_пользователей. В дальнейшем компании будут стремиться предоставлять пользователям больше возможностей самостоятельно определять, какие данные они готовы передавать и разрешать использовать.

Таким образом, особенности бизнес-экосистем создают дополнительные сложности в защите пользовательских данных. Большое количество связанных сервисов и единая система доступа делают использование экосистем удобнее, но при этом повышают риск утечек. Для решения этой проблемы недостаточно только законодательных мер. По этой причине компаниям необходимо контролировать безопасность всех партнёров, соблюдать общие требования к защите информации и не собирать лишние данные. Грамотный подход к информационной безопасности поможет снизить риски и укрепить доверие пользователей.

Список литературы

1. Довжик, В. Н. Цифровые экосистемы: трансформация конкурентных маркетинговых стратегий в российской экономике / В. Н. Довжик, Г. В. Довжик, М. С. Куропаткина // Вестник Южно-Уральского государственного университета. Серия «Экономика и менеджмент». – 2025. – Т. 19, № 3. – С. 186–196. – DOI 10.14529/em250315.

2. Рыжков, Д. А. Вопрос о необходимости урегулирования цифровых экосистем в Российской Федерации / Д. А. Рыжков // Правовая культура в современном обществе. – 2025. – С. 323–325.

3. Anderson, R. The Economics of Information Security / R. Anderson, T. Moore // Science. – 2006. – Vol. 314, No. 5799. – P. 610–613. – DOI 10.1126/science.1130992.

4. Селюк, А. С. Защита персональных данных в цифровом пространстве / А. С. Селюк // Вестник Университета имени О. Е. Кутафина (МГЮА). – 2023. – № 2 (102). – С. 110–119. – DOI 10.17803/2311–5998.2023.102.2.110–119.

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

5. Карунная, Я. А. Проблемы защиты персональных данных в условиях цифровой трансформации / Я. А. Карунная // Юридическая наука и практика. – 2023. – Т. 19, № 3. – С. 47–56. – DOI 10.25205/2542–0410–2023–19–3-47–56.

6. Gordon, L. A. The Economics of Information Security Investment / L. A. Gordon, M. P. Loeb // ACM Transactions on Information and System Security. – 2002. – Vol. 5, No. 4. – P. 438–457. – DOI 10.1145/581271.581274.

7. Роскомнадзор зафиксировал снижение числа утечек персональных данных в 2025 году // ComNews. – 22.01.2026. – URL: https://www.comnews.ru/content/243383/2026–01–22/2026-w04/1009/roskomnadzor-zafiksiroval-snizhenie-chisla-utechek-personalnykh-dannykh-2025-godu (дата обращения: 08.11.2026). – Текст : электронный.

8. Российская Федерация. Законы. О персональных данных: Федеральный закон : от 27.07.2006 №152-ФЗ.

9. Российская Федерация. Законы. О внесении изменений в Кодекс Российской Федерации об административных правонарушениях: Федеральный закон : от 30.11.2024 №420-ФЗ.

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)