Обеспечение конфиденциальности клиентских данных при разработке проектов в условиях цифровизации

С.С. Шишков

Самарский национальный исследовательский университет имени академика С.П. Королева, Самара, Россия

Обоснование. В условиях стремительной цифровой трансформации обеспечение конфиденциальности клиентских данных является важным элементом стратегии развития современного бизнеса. Рост объемов обрабатываемой информации, расширение цифровых каналов взаимодействия с клиентами обусловливает актуальность данной проблемы и особое ее значение в проектной деятельности.

Цель — исследовать инструменты обеспечения конфиденциальности клиентских данных при разработке проектов в условиях цифровизации.

Методы. При исследовании инструментов защиты клиентской информации в процессе разработки проектов использован сравнительный метод, метод графической интерпретации, а также общенаучные методы анализа.

Результаты. В ходе исследования выявлено, что отечественные компании испытывают колоссальное давление со стороны киберпреступности. О росте количества утечек информации в отечественном бизнесе свидетельствуют данные, приведенные на рис. 1 [1].

Согласно официальной статистике, за 2024 год зарегистрировано более 640 тыс. случаев дистанционного мошенничества, общий ущерб от киберпреступлений составил свыше ₽170 млрд [3]. Основные негативные последствия утечки конфиденциальной информации для компаний связаны с прямым финансовым ущербом, потерей доверия клиентов, операционными сбоями, нарушением коммуникаций с партнерами и поставщиками, потерей конкурентных преимуществ и т. д. Это обусловливает особую значимость обеспечения конфиденциальности клиентских данных при разработке проектов. В этой связи наиболее результативным является подход, основанный на гибких технологиях проектного управления Agile, обеспечивающих ситуационное управление по значительным проблемам и отклонениям при утере клиентских данных.

Гибкие технологии управления проектами позволяют использовать современные инструменты обеспечения конфиденциальности клиентских данных. Представляется целесообразным применение таких инструментов защиты клиентской информации, как анонимизация, система безопасности SIEM (Security Information and Event Management), архитектура нулевого доверия (табл. 1).

Анонимизация предполагает полное удаление или необратимое изменение информации, которая позволяет идентифицировать человека, например удаление имен, номеров телефонов или IP-адресов [1]. SIEM системы осуществляют сбор данных из разнородных источников, сетевых устройств, серверов, облачных сервисов, приложений и преобразуют их в единый формат. Это позволяет выявлять аномалии, которые остаются незаметными при ручном анализе [4]. Архитектура нулевого доверия отличается от традиционных

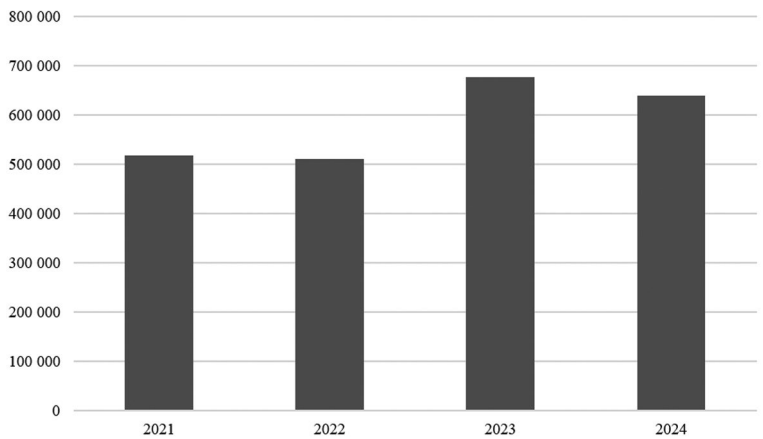

Рис. 1. Количество киберпреступлений в России (2021–2024)

подходов, где доверие распространяется на пользователей и устройства внутри корпоративного периметра. Данная модель требует постоянной проверки подлинности и авторизации для каждого запроса доступа к ресурсам, независимо от его источника [2].

Таблица 1. Характеристика инструментов защиты клиентской информации

Инструменты	Результат применения при разработке проектов
Анонимизация данных	Позволяет аналитикам и менеджерам отслеживать метрики без раскрытия конфиденциальной информации. Защищает конфиденциальные сведения при обмене информацией со стейкхолдерами
SIEM (Security Information and Event Management)	Ускоряет устранение угроз, минимизируя задержки в релизах и обеспечивая стабильность проектных сред. Помогает выявлять уязвимости, оптимизировать процессы и повышать уровень безопасности при разработке проекта
Архитектура нулевого доверия	Обеспечивает безопасный доступ к проектным данным, снижая риск утечек. Позволяет изолировать компоненты проекта, предотвращая распространение угроз и обеспечивая безопасность при обновлениях клиентских данных

Выводы. Проведенный анализ свидетельствует о целесообразности использования при разработке проектов инструментов анонимизации, SIEM-систем и архитектуры нулевого доверия для обеспечения многоуровневой защиты клиентской информации в условиях цифровой трансформации. Гибкие методологии управления проектами Agile, дополненные современными инструментами защиты, минимизируют операционные и репутационные потери при разработке проектов.

Ключевые слова: конфиденциальность данных; цифровизация; киберпреступность; разработка проектов; анонимизация; SIEM-системы; архитектура нулевого доверия.

Список литературы

1. habr.com [Электронный ресурс]. Анонимизация базы данных или как быть уверенным, что ты не нарушаешь закон «О персональных данных». Режим доступа: https://habr.com/ru/articles/654719/ Дата обращения: 17.05.2025.
2. kaspersky.ru [Электронный ресурс]. Концепция безопасности Zero Trust: преимущества и принцип работы. Режим доступа: https://www.kaspersky.ru/resource-center/definitions/zero-trust Дата обращения: 17.05.2025.
3. clck.ru [Электронный ресурс]. Число киберпреступлений в России. Режим доступа: https://clck.ru/3M83NZ Дата обращения: 17.05.2025.
4. cloudnetworks.ru Security Information and Event Management. Режим доступа: https://cloudnetworks.ru/inf-bezopasnost/siem-log-management/ Дата обращения: 17.05.2025.

Сведения об авторе:

Сергей Сереевич Шишков — студент, группа 7421-380302D, институт экономики и управления; Самарский национальный исследовательский университет имени академика С.П. Королева, Самара, Россия. E-mail: xipleeee@yandex.ru

Сведения о научном руководителе:

Тамара Борисовна Заводчикова — кандидат экономических наук; доцент кафедры общего и стратегического менеджмента; Самарский национальный исследовательский университет имени академика С.П. Королева, Самара, Россия. E-mail: toma.zavod@gmail.com