УДК 004.056.5:658.62

Оценка эффективности внедрения Zero Trust в российском e-commerce

В.Э. Марушевский✉

Национальный исследовательский университет ИТМО, Санкт-Петербург, Россия

В статье рассмотрены актуальные проблемы внедрения модели Zero Trust в России в условиях роста киберугроз и ужесточения требований к защите данных. Исследованы ключевые барьеры, включая стандартизированные метрики оценки эффективности и необходимость адаптации международных фреймворков к российскому нормативному контексту и сложности интеграции в бизнес-процессы. Проанализированы релевантные показатели. Особое внимание уделено влиянию Zero Trust на пользовательский опыт и бизнес-результаты e-commerce-компаний.

Ключевые слова: Zero Trust, информационная безопасность, электронная коммерция, киберугрозы, метрики эффективности, микросегментация.

Evaluation of the Effectiveness of the Implementation of Zero Trust in Russian E-commerce

V.E. Marushevsky✉

ITMO University, Saint Petersburg, Russia

The article discusses the current problems of implementing the Zero Trust model in Russia in the context of increasing cyber threats and stricter data protection requirements. The key barriers are investigated, including standardized performance assessment metrics and the need to adapt international frameworks to the Russian regulatory context and the complexity of integration into business processes. Relevant indicators are analyzed. Special attention is paid to the impact of Zero Trust on the user experience and business results of e-commerce companies.

Keywords: Zero Trust, information security, e-commerce, cyber threats, performance metrics, microsegmentation.

В условиях стремительного роста цифровой экономики и увеличения объема обрабатываемых персональных и финансовых данных электронная коммерция в России сталкивается с новыми вызовами в области информационной безопасности. Множественные инциденты, связанные с утечками данных, фишингом, компрометацией учетных записей и другими видами киберугроз (рис. 1) [1], подчеркивают необходимость пересмотра традиционных подходов к защите информационных систем.

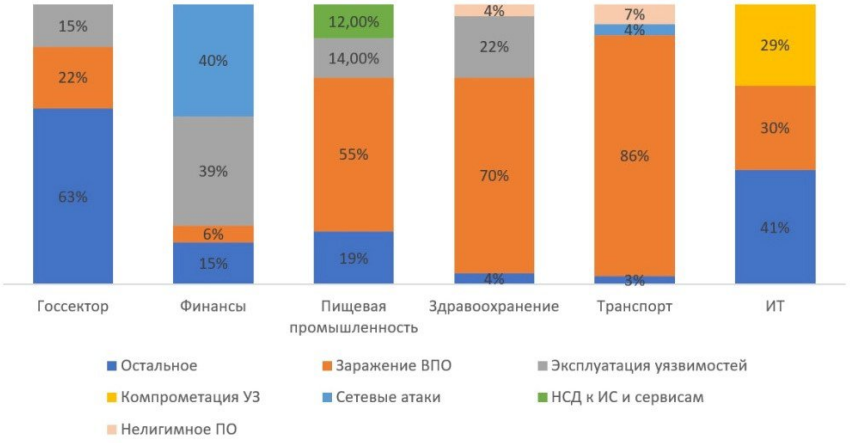

Рисунок 1. Распределение инцидентов по отраслям в России

Одной из наиболее прогрессивных концепций в сфере кибербезопасности является модель Zero Trust, основанная на принципах отказа от доверия к любым пользователям и устройствам внутри и вне периметра сети. Данная модель активно развивается на международной арене и рассматривается как эффективный механизм противодействия современным угрозам. Однако несмотря на концептуальное признание Zero Trust как перспективного подхода, в российском контексте, особенно в сегменте e-commerce, остаются нерешёнными ключевые вопросы, касающиеся оценки его эффективности.

В контексте электронной коммерции наиболее уязвимыми зонами для реализации принципов Zero Trust являются клиентские веб-интерфейсы, API-интеграции с внешними поставщиками и платформы персонализации, активно обрабатывающие поведенческие данные пользователей. Именно в этих точках происходит наиболее частое нарушение принципа наименьших привилегий и отсутствует полноценная проверка подлинности и авторизации на каждом этапе транзакции.

Несмотря на активное развитие концепции Zero Trust и её признание как одного из наиболее перспективных подходов к обеспечению информационной безопасности, в российских отраслях остается ряд нерешённых проблем, препятствующих объективной оценке эффективности её внедрения и стоящих на ряду с барьерами внедрения Zero Trust (рис. 2) [4].

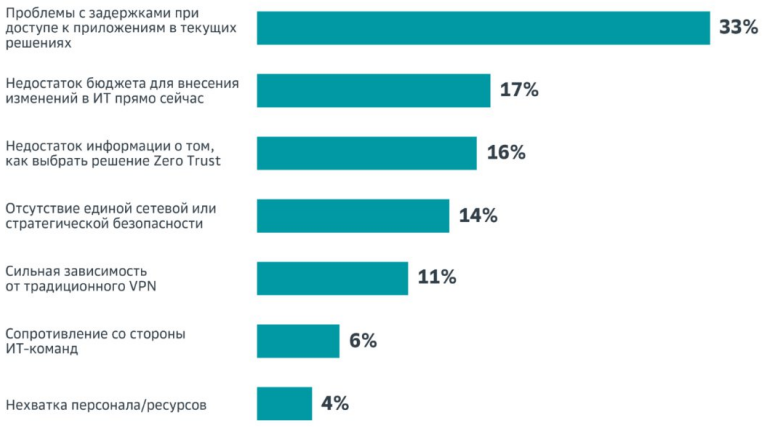

Рисунок 2. Барьеры внедрения Zero Trust

Одним из ключевых барьеров является отсутствие унифицированных метрик, позволяющих формализованно измерять влияние Zero Trust на защищённость инфраструктуры, устойчивость к инцидентам, а также на бизнес-показатели компании. В отличие от более зрелых зарубежных рынков, в российской практике нет согласованных критериев, с помощью которых можно было бы проводить оценку как на уровне отдельных компонентов (аутентификация, микросегментация, мониторинг), так и на уровне всей архитектуры безопасности.

Кроме того, международные методики и фреймворки, такие как Forrester Zero Trust eXtended (ZTX) или NIST SP 800-207, не всегда применимы в российском контексте. Их применение требует адаптации под действующее законодательство, включая требования по обработке персональных данных, хранению информации и выполнению предписаний регуляторов – в первую очередь ФСТЭК и Роскомнадзора [3]. Таким образом, даже в случае технической реализации Zero Trust, компании сталкиваются с трудностями в формировании методической базы для оценки достигнутых результатов.

Дополнительную сложность представляет интеграция метрик Zero Trust в существующие бизнес-процессы e-commerce-компаний. Из-за высокой динамики рынка, множества подрядчиков, сложной ИТ-инфраструктуры и разнообразных каналов взаимодействия с пользователями, внедрение модели нулевого доверия требует глубокой трансформации процессов. Это, в свою очередь, делает затруднительным измерение эффективности на ранних этапах внедрения и повышает риски субъективных трактовок полученных результатов.

Наконец, остаётся неопределённым влияние Zero Trust на пользовательский опыт и ключевые бизнес-показатели – такие как конверсия, отказоустойчивость и скорость обработки заказов. Без чётких количественных ориентиров компании оказываются перед дилеммой: с одной стороны, усиливаются меры контроля и безопасности, с другой – потенциально возрастает фрустрация пользователей и снижается удобство взаимодействия. В совокупности это формирует существенный научно-практический пробел, требующий разработки адаптированной системы оценки, ориентированной на специфику российского e-commerce.

Несмотря на растущий интерес к концепции Zero Trust в России и отдельные кейсы внедрения в крупном бизнесе, в сфере электронной коммерции сохраняется ряд существенных барьеров, мешающих объективной оценке эффективности этой модели.

Дополнительную сложность представляет ограниченная применимость международных методик. Такие фреймворки, как Forrester ZTX или NIST SP 800-207, ориентированы на рынки с иными нормативными реалиями и зачастую не учитывают специфические требования российского законодательства в области обработки персональных данных, хранения информации и взаимодействия с регуляторами. Их прямое копирование без адаптации не только неэффективно, но и может быть юридически рискованным. Кроме того, сложность интеграции даже адаптированных метрик в бизнес-процессы электронной коммерции – с их высокой динамикой, большим числом подрядчиков и разнообразием цифровых каналов – затрудняет внедрение модели Zero Trust как управляемой системы с измеримыми показателями эффективности.

Анализ существующих международных метрик позволяет выделить наиболее релевантные из них, которые потенциально могут быть адаптированы для применения в российском контексте. Прежде всего, это показатели, связанные с управлением инцидентами, отраженные в таблице.

Таблица

Ключевые метрики для оценки эффективности внедрения Zero Trust

Метрика	Описание	Использование
MTTD / MTTR	Время на обнаружение и реагирование на угрозы	Оценка скорости и эффективности реагирования
Количество инцидентов	Общее число атак / попыток вторжения	Показатель уязвимости и эффективности защиты
Доля избыточных прав	Пользователи с доступом выше необходимого	Проверка соблюдения принципа минимальных привилегий
Степень внедрения MFA	Процент пользователей с многофакторной аутентификацией	Базовый элемент Zero Trust
Сегментация сети	Наличие зон безопасности, ограниченного доступа	Ограничение распространения угроз
Число утечек данных	Случаи компрометации информации	Ключевой индикатор защищённости
Уровень зрелости ZT	Общая степень реализации Zero Trust по модели / чек-листу	Помогает понять текущую позицию и спланировать развитие

Представленные метрики в таблице демонстрируют как техническую, так и бизнес-ориентированную направленность подхода Zero Trust. Однако при их адаптации к условиям российского e-commerce следует учитывать специфику:

– наличие нормативных ограничений на обработку персональных данных;
– низкий уровень зрелости процессов в части IAM (управления доступом);
– ограниченность отечественных решений по поведенческой аналитике.

Метрики, связанные с отслеживанием поведения пользователей и микросегментацией, требуют пересмотра или локализации с учетом доступных ИТ-ресурсов.

Внедрение Zero Trust позволяет за счёт микросегментации и постоянного мониторинга существенно сократить данные значения, что особенно важно для e-commerce, где информационная безопасность непосредственно влияет на лояльность клиентов и деловую репутацию.

Также значимыми являются метрики, отражающие снижение числа утечек данных и попыток несанкционированного доступа. Исследования ведущих ИБ-компаний, таких как Cisco и Kaspersky Lab, подтверждают эффективность Zero Trust в этом направлении, однако в российской практике такие показатели, как правило, не агрегируются и редко входят в регулярную отчётность.

В международной практике активно используются комплексные индексы зрелости Zero Trust, включающие уровень внедрения многофакторной аутентификации, охват сетевой сегментацией, полноту журналирования и аудита. Подобные подходы позволяют сформировать общую карту текущего состояния и определить приоритетные зоны развития. В российских условиях, несмотря на отсутствие официальных аналогов, элементы этих методик находят отражение в отраслевых отчётах и рекомендациях регуляторов.

Концепция Zero Trust обладает значительным потенциалом для повышения информационной безопасности в российском сегменте электронной коммерции, однако

её эффективное внедрение требует преодоления ряда методологических и практических барьеров. Ключевыми проблемами остаются отсутствие унифицированных оценочных показателей, необходимость адаптации международных стандартов к российскому нормативному контексту, а также сложности интеграции в существующие бизнес-процессы без ущерба для пользовательского опыта.

Перспективы развития Zero Trust в России связаны с разработкой специализированных метрик оценки, учитывающих как технические аспекты безопасности, так и бизнес-показатели электронной коммерции. Важным направлением является создание адаптированных методик на основе международного опыта, которые позволят объективно оценивать эффективность модели применительно к отечественной ИТ-инфраструктуре и регуляторным требованиям.

СПИСОК ИСТОЧНИКОВ

1. Кибератаки на российские компании в 2024 году – отчет Solar JSOC // Solar [Электронный ресурс]. – 2015. – URL: https://rt-solar.ru/analytics/reports/5320/ (дата обращения: 26.03.2025).

2. Never trust, always verify: The Zero Trust security model: What is Zero Trust, and why is it attractive for modern business? // Kaspersky Official Blog [Электронный ресурс]. – URL: https://www.kaspersky.com/blog/zero-trust-security/36423/ (дата обращения: 26.03.2025).

3. Иванов П.А. Модель реализации управления доступом к информационным активам в концепции нулевого доверия / П.А. Иванов, И.В. Капгер, А.С. Шабуров // Вестник ПНИПУ. Электротехника, информационные технологии, системы управления. – 2023. – № 45. – С. 147–163.

4. Теорема зеро. Почему концепция нулевого доверия всё более популярна // СберПро [Электронный ресурс]. – URL: https://sber.pro/publication/teorema-zero-pochemu-kontseptsiya-nulevogo-doveriya-vsyo-bolee-populyarna/ (дата обращения: 26.03.2025).

5. Актуальные киберугрозы в ритейле // Positive Technologies [Электронный ресурс]. – 2002. – URL: https://ptsecurity.com/ru-ru/research/analytics/retail-cybersecurity-threatscape-2023/ (дата обращения: 26.03.2025).

6. Цифровые технологии и проблемы информационной безопасности / Т.И. Абдуллин, В.Д. Баев, М.В. Буйневич [и др.]; под ред. Е.В. Стельмашонок, И.Н. Васильевой. – Санкт-Петербург: Издательство Санкт-Петербургского государственного экономического университета, 2021. – 163 с.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Марушевский Вадим Эдуардович, студент, Национальный исследовательский университет ИТМО, Санкт-Петербург, Россия.
e-mail: vadik.marushevsckyw@yandex.ru