МОДЕЛЬ АНАЛИЗА ЧУВСТВИТЕЛЬНОСТИ БИЗНЕС-ПРОЦЕССОВ К КОМПЬЮТЕРНЫМ АТАКАМ (НА ПРИМЕРЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ПРОДАЖИ ЖЕЛЕЗНОДОРОЖНЫХ БИЛЕТОВ)

А.В. Горелик, *д-р техн. наук, профессор*
А.Д. Репин, *магистр*
Российский университет транспорта (МИИТ)
(Россия, г. Москва)

DOI:10.24412/2500-1000-2025-10-2-30-35

Аннотация. *В статье рассматривается модель анализа чувствительности бизнес-процессов к компьютерным атакам на примере автоматизированной системы продажи железнодорожных билетов (АС ПЖБ). Цель работы – изучение практической возможности применение модели для оценки степени уязвимости ключевых процессов (сервисов) к различным типам кибератак, а также оценки их последствий. Рассмотрены этапы построения модели: определение бизнес-процессов, идентификация информационных активов, определение наиболее вероятных кибератак, количественная оценка чувствительности процессов с использованием показателей вероятности и последствий угроз. По результатам проведённого анализа разработан перечень мероприятий по повышению устойчивости бизнес-процессов АС ПЖБ к компьютерным атакам.*

Ключевые слова: *бизнес-процессы, анализ чувствительности, кибератаки, онлайн-платежи, модель устойчивости, DDoS; SIEM; SOC.*

В современном мире всеобщая цифровизация привела к значительному росту уязвимостей, связанных с компьютерными атаками. Понимание того, как различные бизнес-процессы реагируют на такие угрозы, становится ключевым фактором обеспечения стабильности и безопасности [1].

Увеличение количества цифровых сервисов в транспортной инфраструктуре, включающих в себя огромное количество бизнес-процессов, является неотъемлемым фактором развития отрасли. Наиболее востребованным сервисом является автоматизированная продажа билетов, который подвержен воздействию различных киберугроз. Нарушение работы сервиса в результате кибератак может привести к серьёзным экономическим потерям, социальным сбоям и падению доверия пользователей. Актуальными задачами являются выявление наиболее критичных бизнес-процессов в АС ПЖБ и разработка мер по их защите.

Модель анализа чувствительности бизнес-процессов к компьютерным атакам – это прежде всего структурированный подход, позволяющий провести оценку степени уязвимости ключевых процессов к различным типам кибератак, а также оценить их последствия [2]. Такая модель обычно объединяет методы риск-менеджмента, анализа бизнес-процессов и информационной безопасности.

К основным элементам модели относятся:

1. Определение бизнес-процессов. Производится идентификация критичных процессов и определяются их роли, осуществляется построение схемы взаимосвязей между процессами [1].

2. Идентификация информационных активов. Осуществляется выделение ключевых ИТ-систем, приложений, баз данных, коммуникационных каналов, на которых базируется каждый процесс, установление критичности активов [3].

3. Определение возможных кибератак. Для каждой атаки определяется вероятность реализации и потенциальный ущерб (финансовый, репутационный, юридический) [4].

4. Оценка чувствительности процессов к компьютерным атакам и разработка мер по повышению их устойчивости [2, 5].

В АС ПЖБ выделяются следующие ключевые бизнес-процессы:

1. Онлайн-продажа билетов (веб-сайт, мобильное приложение).

2. Оформление билетов в кассах и терминалах самообслуживания.

3. Обработка платежей (интеграция с банками и шлюзами).

4. Резервирование мест в поездах.

5. Формирование отчётности (финансовой и статистической).

6. Поддержка клиентов (колл-центр, чат-боты).

Ключевые бизнес-процессы имеют логические связи. Клиенты взаимодействуют с онлайн-продажей и кассами. Оба канала обращаются к резервированию мест. Все операции проходят через обработку платежей. Формирование отчётности получает данные из всех процессов. Поддержка клиентов обслуживает инциденты, связанные с любым процессом. Схема бизнес-процессов представлена на рисунке 1.

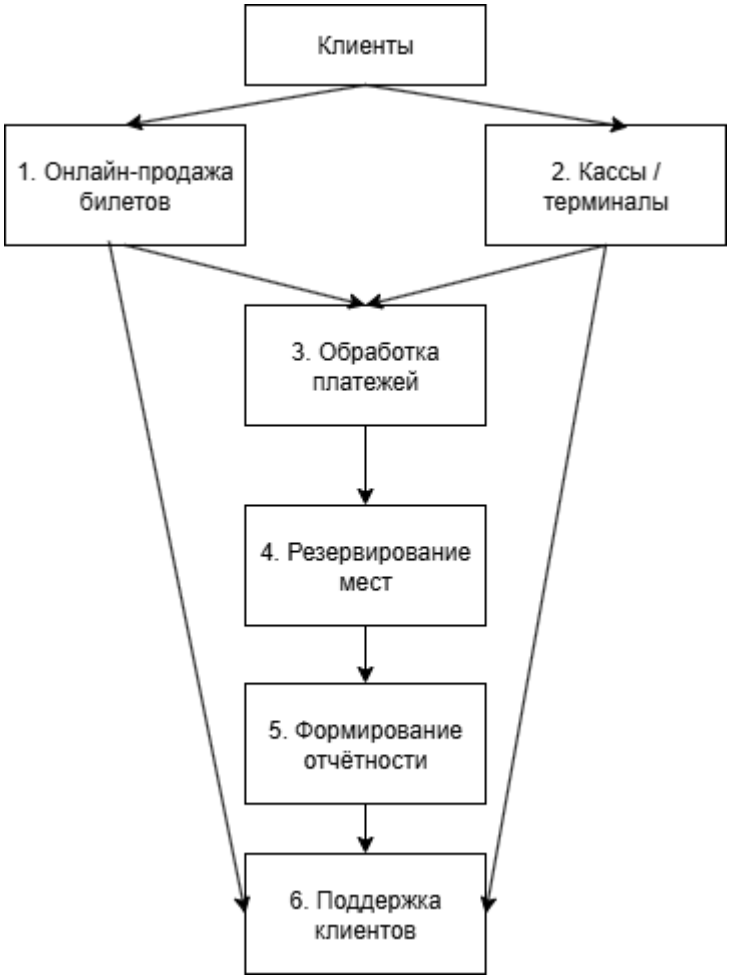

Рис. 1. Схема бизнес-процессов АС ПЖБ

На основании исследований киберугроз в транспортной отрасли, проводимых компанией Positive Technologies, транспортный сектор привлекают внимание злоумышленников, как политически, так и финансово мотивированных, и являются одной из основных целей кибератак [6]. Так, функционирование автоматизированной системы продажи железнодорожных билетов сопряжено с воздействием различных киберугроз, а именно:

DDoS-атаки – перегрузка серверов с помощью ботнетов, генерация «мусорного» трафика, атаки на уровень приложений (L7). Наиболее опасны в часы пик и в периоды массовых продаж (праздники, отпускной сезон). Последствия DDoS-атаки – отказ в обслуживании онлайн-сервисов, невозможность покупки билетов, потеря выручки, массовое недовольство клиентов, падение репутации компании перевозчика.

Взлом баз данных – SQL-инъекции, эксплуатация уязвимостей веб-приложений, подбор паролей администраторов, атаки на каналы связи. Базы содержат персональные данные (ФИО, паспортные данные, реквизиты банковских карт), а также критическую бизнес-информацию о пассажиропотоке. Последствия взлома баз данных – массовые утечки,

штрафы за нарушение законодательства, утрата доверия пассажиров, возможное мошенничество с использованием украденных данных [3].

Вредоносное программное обеспечение – внедрение вирусов, троянов, программ-вымогателей, использование заражённых носителей или фишинговых вложений. Заражение серверов может привести к остановке биллинга, искажению расписания, подмене цен и маршрутов. Последствия воздействия вредоносного программного обеспечения – полный отказ системы, блокировка серверов, финансовые и организационные потери.

Фишинг и социальная инженерия – рассылка поддельных писем, создание сайтов-клонов систем продажи билетов, телефонные звонки от имени службы поддержки. Как правило пользователи массово вводят свои данные на фишинговых ресурсах, особенно в период активных продаж. Последствия фишинга и социальной инженерии – кража учётных данных и реквизитов карт, прямые финансовые потери клиентов, снижение доверия к перевозчику, рост числа жалоб.

Инсайдерские угрозы – действия сотрудников (кассиров, администраторов, операторов), обладающих доступом к данным и системам. Возможны несанкционированные возвраты билетов, изменение данных о пассажирах и маршрутах, продажа информации злоумышленникам. Последствия Инсайдерской угрозы – мошенничество, утечки персональных данных, прямой ущерб компании, репутационные потери.

Для оценки чувствительности бизнес-процессов к кибератакам используется количественная модель на основе формулы:

$$R=P\times I,$$

где R (Risk) – интегральный показатель чувствительности процесса к угрозе, P (Probability) – вероятность реализации угрозы (от 0 до 1), определяется на основе статистики инцидентов, экспертной оценки и анализа уязвимостей, I (Impact) – влияние угрозы на бизнес-процесс (от 0 до 1), отражает масштаб последствий: финансовых, репутационных, юридических [4]. Для повышения точности в базовой модели могут быть добавлены время восстановления процесса и наличие защитных мер, например,

$$R=P\times I\times T\times E,$$

где T – время восстановления, E – наличие защитных мер.

В качестве критерия оценки могут применяться следующие показатели.

Вероятность (P):

0.1–0.3 → низкая (редкие атаки).

0.4–0.6 → средняя (фиксируются периодически).

0.7–1.0 → высокая (угроза актуальна постоянно).

Влияние (I):

0.1–0.3 → ограниченный ущерб, затрагивает отдельные подразделения.

0.4–0.6 → значимые потери, нарушение работы части сервисов.

0.7–1.0 → критические последствия: остановка ключевых функций, финансовые потери, кризис доверия.

Чувствительность процесса (R):

$R > 0,7$ → высокая чувствительность.

$0,4 < R < 0,7$ → средняя чувствительность.

$R < 0,4$ → низкая чувствительность.

Соответственно несложно произвести оценки чувствительности всех указанных бизнес-процессов. Так, например, при оценке чувствительности онлайн-продаж билетов при воздействии DDoS атак необходимо учитывать следующие показатели: вероятность P = 0.9 (атаки происходят часто), влияние I = 1.0 (отказ сервиса полностью останавливает продажи).

$$R = 0.9 \times 1.0 = 0.9 \text{ (критический уровень).}$$

При оценке чувствительности бизнес-процессов отчётность при инсайдерах необходимо учитывать следующие показатели: вероятность P = 0.5 (возможность злоупотреблений средняя), I = 0.5 (искажение отчётности ведёт к юридическим рискам, но не останавливает продажи).

$$R = 0.5 \times 0{,}5 = 0.25 \text{ (низкий уровень).}$$

Результаты оценки чувствительности бизнес-процессов АС ПЖБ к воздействию к компьютерным атакам представлены в таблице 1.

Таблица 1. Оценки чувствительности бизнес-процессов к кибератакам

Процесс / Угроза	DDoS	Взлом БД	Вредоносное ПО	Фишинг	Инсайдеры
Онлайн-продажа	0.9	0.7	0.6	0.7	0.5
Платежи	0.9	0.7	0.6	0.7	0.5
Резервирование мест	0.72	0.56	0.48	0.56	0.40
Кассы	0.63	0.49	0.42	0.49	0.35
Отчётность	0.45	0.35	0.30	0.35	0.25

Пример оценки чувствительности бизнес-процессов АС ПЖБ к кибератакам представлен на рисунке 2.

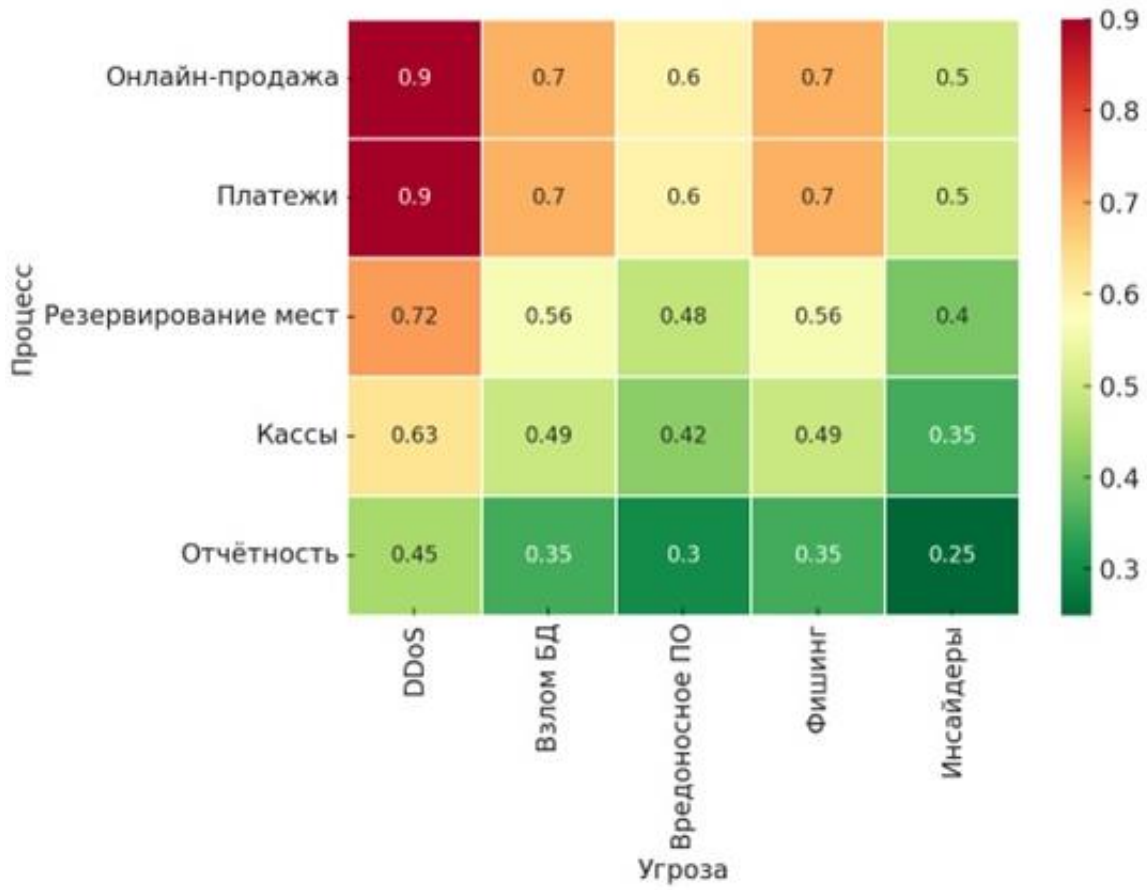

Рис. 2. Пример оценки чувствительности бизнес-процессов АС ПЖБ к кибератакам

Где красные зоны – высокая чувствительность, жёлтые зоны – средняя чувствительность, зелёные зоны – низкая чувствительность [7, 8].

Проведённый анализ показал, что бизнес-процессы автоматизированной системы продажи железнодорожных билетов имеют разную степень чувствительности к компьютерным атакам. Наибольшую критичность демонстрируют онлайн-продажа билетов и обработка платежей. Среднюю чувствительность показали процессы резервирования мест и кассового обслуживания, где атаки приводят к нарушению логистики и отдельным случаям мошенничества. Наименее уязвимым оказался процесс формирования отчётности. Таким образом, наиболее уязвимыми являются процессы, напрямую связанные с клиентами и денежными транзакциями. Они должны быть приоритетными для инвестиций в защиту и мониторинг.

По результатам проведённого анализа разработан перечень мероприятий по повышению устойчивости бизнес-процессов АС ПЖБ к компьютерным атакам, а именно:

1. Защита от DDoS-атак - использовать специализированные сервисы фильтрации трафика, применять балансировку нагрузки и георазпределённые серверные кластеры, обеспечивать автоматическую блокировку подозрительных запросов.

2. Защита баз данных (от взлома и утечек) – применять шифрование данных, обеспечивать разграничение прав доступа, использовать WAF (Web Application Firewall) против SQL-инъекций и XSS-атак, регулярно проводить тесты на проникновение и аудит безопасности [9].

3. Противодействие вредоносному ПО – обеспечивать сегментацию сети и централизованную антивирусную защиту с EDR (Endpoint Detection and Response), использовать «песочницы» для анализа вложений и подозрительных файлов, обеспечивать регулярное обновление ПО.

4. Защита от фишинга – внедрять антифишинговые фильтры и двухфакторную аутентификацию для всех сотрудников, обучать персонал распознаванию фишинговых писем и сайтов, использовать DMARC/DKIM/SPF для защиты домена от подделки.

5. Инсайдерские угрозы (сотрудники касс, администраторы) – разграничивать права и обеспечивать журналирование действий сотрудников, внедрять системы DLP (Data Loss Prevention) для контроля передачи данных, обеспечивать мониторинг (вовремя выявлять риски злоупотреблений).

При этом необходимо обратить внимание на реализацию общих мер по повышению устойчивости, к которым можно отнести: создание и обучение SOC (Security Operations Center) для мониторинга и реагирования на инциденты, внедрение системы SIEM для централизованного сбора и анализа логов, разработка плана реагирования на инциденты (IRP – Incident Response Plan, проведение регулярных киберучений (Red Team vs Blue Team) [8].

Таким образом, построенная модель анализа чувствительности бизнес-процессов АС ПЖБ к компьютерным атакам:

- обеспечивает количественную оценку угроз и последствий [2, 5];
- позволяет выявить наиболее уязвимые процессы и определить «узкие места» инфраструктуры;
- служит инструментом для приоритизации инвестиций в средства информационной безопасности;
- способствует формированию стратегии киберустойчивости транспортной компании [10].

Применение данной модели в транспортной отрасли позволяет повысить защищённость ключевых цифровых сервисов, обеспечить непрерывность работы систем продажи билетов и укрепить доверие пассажиров.

Библиографический список

1. ISO/IEC 27001:2013. Системы менеджмента информационной безопасности. – Женева: ISO/IEC, 2013.

2. ISO/IEC 27005:2018. Управление рисками информационной безопасности. – Женева: ISO/IEC, 2018.

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

4. IBM. Индекс угроз информационной безопасности IBM X-Force Threat Intelligence Index 2023. – Нью-Йорк: IBM Corporation, 2023. – [Электронный ресурс]. – Режим доступа: https://www.ibm.com/xforce-threat-intelligence-index.

5. NIST SP 800-30 Rev. 1. Руководство по проведению оценки рисков. – Гейтерсбург: NIST, 2012.

6. Positive Technologies. Киберугрозы в транспортной отрасли. – [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cyber-threats-in-the-transport-sector-2023/.

7. NIST SP 800-61 Rev. 2. Руководство по обработке инцидентов компьютерной безопасности. – Гейтерсбург: NIST, 2012.

8. Gartner. Глобальное исследование рынка центров обеспечения безопасности (Market Guide for Security Operations Centers). – Сентябрь 2022.

9. Приказ ФСТЭК России № 239 от 20.12.2021 г. «Об утверждении требований к защите информации в государственных информационных системах».

10. ISO/IEC 22301:2019. Системы менеджмента непрерывности бизнеса. – Женева: ISO/IEC, 2019.

MODEL OF SENSITIVITY ANALYSIS OF BUSINESS PROCESSES TO CYBER ATTACKS (CASE STUDY OF AUTOMATED RAILWAY TICKETING SYSTEM)

A.V. Gorelik, *Doctor of Technical Sciences, Professor*
A.D. Repin, *Master*
Russian University of Transport (MIIT)
(Russia, Moscow)

Abstract. *The article examines a sensitivity analysis model for business processes exposed to cyber attacks using the automated railway ticketing system (ARTS) as a case study. The aim of the study is to explore the practical applicability of the model for assessing the vulnerability level of key processes (services) to various types of cyber attacks, as well as for evaluating their potential impacts. The paper describes the stages of model development, including the identification of business processes, recognition of information assets, determination of the most probable cyber attacks, and a quantitative assessment of process sensitivity using threat probability and impact indicators. Based on the analysis results, a set of measures was developed to enhance the resilience of ARTS business processes against cyber attacks.*

Keywords: *business processes, sensitivity analysis, cyber attacks, online payments, resilience model, DDoS, SIEM, SOC.*