

Челак Светлана Васильевна, к.э.н., доцент
Санкт-Петербургский государственный экономический университет
Chelak Svetlana Vasilievna
candidate of Economic Sciences, Associate Professor, SPbGEU

Вдовиченко Степан Андреевич, студент
Санкт-Петербургский государственный экономический университет
Vdovichenko Stepan Andreevich, student, SPbGEU

**СОВЕРШЕНСТВОВАНИЕ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ ТЕАТРАЛЬНОЙ ОРГАНИЗАЦИИ
КАК ФАКТОР ЭКОНОМИЧЕСКОЙ УСТОЙЧИВОСТИ
(НА ПРИМЕРЕ ООО «ТВОРЧЕСКОЕ ОБЪЕДИНЕНИЕ «ТЕАТРОМ»)
IMPROVING THE INFORMATION SECURITY OF A THEATRICAL ORGANIZATION
AS A FACTOR OF ECONOMIC SUSTAINABILITY (ON THE EXAMPLE
OF THE CREATIVE ASSOCIATION «TEATRDOM»)**

Аннотация. В статье рассматривается роль информационной составляющей в системе экономической безопасности театральной организации на примере ООО «Творческое объединение «ТеатрДом». Анализируются специфические угрозы информационной безопасности в сфере исполнительских искусств. Обосновывается, почему информационная безопасность становится критически важным фактором устойчивости современного театрального бизнеса.

Abstract. The article examines the role of the information component in the economic security system of a theater organization on the example of LLC Creative Association TeatrDom. Specific threats to information security in the field of performing arts are analyzed. It is substantiated why information security is becoming a critical factor in the sustainability of the modern theater business.

Ключевые слова: Информационная безопасность, экономическая безопасность, театральная организация, билетные системы, персональные данные, кадровая безопасность, репутационные риски.

Keywords: Information security, economic security, theater organization, ticket systems, personal data, personnel security, and reputational risks.

В современном мире информация стала одним из ключевых активов любой организации, а её защита – неотъемлемым условием экономической устойчивости [1]. Для театральной организации, которую многие продолжают воспринимать исключительно как «храм искусства», вопросы информационной безопасности долгое время оставались на периферии управленческого внимания. Однако сегодня, когда театры активно – продают билеты онлайн, ведут электронные базы зрителей, используют облачные сервисы для документооборота и осуществляют финансовые транзакции через интернет – информационная безопасность становится критически важным элементом экономической безопасности.

Цель данной статьи – показать, зачем театральной организации (и в частности, ООО «Творческое объединение «ТеатрДом») нужна информационная составляющая экономической безопасности, с чем она экономически переплетается и на какие аспекты деятельности влияет.

Информационная безопасность – это защита информации и поддерживающей её инфраструктуры от любых воздействий, результатом которых может явиться нанесение ущерба конфиденциальности, целостности и доступности информации. Однако для театральной организации это определение требует конкретизации [2, с. 173].



Какая информация в театре нуждается в защите? Это, как минимум: персональные данные зрителей (при продаже билетов онлайн и в кассах); персональные данные сотрудников; билетные системы и данные о продажах; договорная база с контрагентами (площадками, артистами, подрядчиками); финансовая документация и банковские транзакции; интеллектуальная собственность (фотографии спектаклей, описание спектаклей, товарный знак театра); внутренняя переписка и документооборот.

Современный театр – это бизнес со значительными денежными потоками [3, с. 20]. Продажа билетов онлайн, использование «Пушкинской карты», оплата через терминалы – всё это создаёт точки уязвимости. По данным экспертов, билетные системы становятся «узким местом», через которое проходят потоки культурной активности и финансовые показатели. Когда билетный сервис работает без должного уровня безопасности, театр рискует столкнуться сразу с несколькими неприятными сценариями. Уязвимости открывают дорогу мошенникам, провоцируют сбои в учёте проданных мест и могут в любой момент вывести из строя кассовое оборудование. А это, в свою очередь, «бьёт по кассе» – в прямом смысле слова, потому что зрительские деньги уходят мимо или вовсе теряются в запутанных возвратах.

Ещё одна проблема – сайты-клоны. Мошенники создают страницы-подделки под видом официальных площадок театра, где билеты стоят в разы дороже, а иногда их просто не существует. В итоге зритель попадает впросак, теряет деньги и обижается уже на настоящий театр, который к этому мошенничеству никакого отношения не имеет. Репутация в таких историях страдает не меньше, чем бюджет.

Цифровая инфраструктура для театра сейчас – это не просто удобство, а основа для нормальной работы. Если в системе случается сбой, под удар попадают ключевые процессы: приём платежей, учёт зрителей, финансовые транзакции. Без рабочих IT-решений даже хорошо подготовленный спектакль рискует оказаться под угрозой срыва – особенно если речь идёт о вечернем показе, когда потоки людей большие, а время на решение проблем нет [4].

Для ООО «ТеатрДом», у которого несколько сценических площадок, задача усложняется вдвойне. Все филиалы должны обмениваться информацией в реальном времени – иначе данные «разъезжаются», продажи дублируются, а руководство не видит общей картины.

Важно, чтобы на всех уровнях системы действовали прозрачные правила: единый подход к учёту билетов, понятная схема подтверждения операций, надёжные способы проверки пользователей, защита от случайной или намеренной двойной оплаты. И, конечно, стабильный доступ к сервисам в любой момент – чтобы зрители могли купить билет, когда захотят, а театр – получить деньги без задержек и лишних вопросов.

Без надлежащей информационной безопасности операционная деятельность театра становится уязвимой для сбоев, которые могут привести к отмене спектаклей, конфликтам со зрителями и финансовым потерям.

Современный зритель привык покупать билеты онлайн. Если система продаж ненадёжна или сайт театра похож на мошеннический (либо существуют сайты-двойники), зритель может либо отказаться от покупки, либо попасться на уловку мошенников.

Как отмечают эксперты, злоумышленники активно используют поддельные интернет-страницы, маскирующиеся под сайты театров, концертов и выставок [5]. Хотя в 2025 году количество таких фишинговых сайтов сократилось (с 642 до 92 за летние месяцы), проблема не исчезла полностью – мошенники переключились на более изощрённые методы: целевые атаки, дипфейки, взлом аккаунтов в социальных сетях.

Информационная безопасность напрямую влияет на: доверие зрителей к театру; защиту зрителей от мошенников (и, соответственно, сохранение их лояльности); полноту и достоверность учёта проданных билетов; отсутствие двойных продаж и конфликтов в зале.

Театр работает с множеством контрагентов: площадками, артистами, режиссёрами, художниками, подрядчиками. Утечка информации о коммерческих условиях договоров может привести к потере конкурентных преимуществ, конфликтам с партнёрами и юридическим проблемам.



Особую важность приобретает защита интеллектуальной собственности театра. Как показывает практика Театра кукол Образцова, театры могут использовать факты использования их интеллектуальной собственности для борьбы с мошенниками и сайтами-двойниками, требуя компенсации в порядке гражданского законодательства. Это возможно только при условии, что сама интеллектуальная собственность должным образом защищена и учтена.

Информационная безопасность влияет на качество управленческих решений. Если данные искажены или недоступны, руководитель не может адекватно оценить ситуацию.

Список литературы:

1. Нюансы организации информационной безопасности в музеях // Режим доступа: <https://www.secuteck.ru/articles/nyuansy-organizacii-informacionnoj-bezopasnosti-v-muzeyah> (дата обращения 15.06.2026)
2. Абанкина Т.В. Креативные компетенции и интеллектуальная собственность при переходе к инновационной экономике // Трансформация сферы интеллектуальной собственности в современных условиях. Москва: Федеральный институт промышленной собственности, 2020. С. 171-176.
3. Астафьева О.Н. Российская культура в контексте динамики экономических стратегий / О.Н. Астафьева, И.В. Малыгина // Вестник Московского государственного университета культуры и искусств. 2022. №4 (108). С. 15-26
4. Информационная безопасность музеев и других объектов культуры // Методические рекомендации, 2025 // Режим доступа: https://www.hermitagemuseum.org/uploads/files/file_file_informatsionnaya_bezopasnost.pdf (дата обращения 15.06.2026)
5. Методические рекомендации по работе с автоматизированной информационной системой «Культурный регион» // Режим доступа: https://tmckrasnoe.ru/uploads/file/dokumevt/Kulturniy_region.pdf (дата обращения 14.06.2026)

