Санкт-Петербургский государственный университет

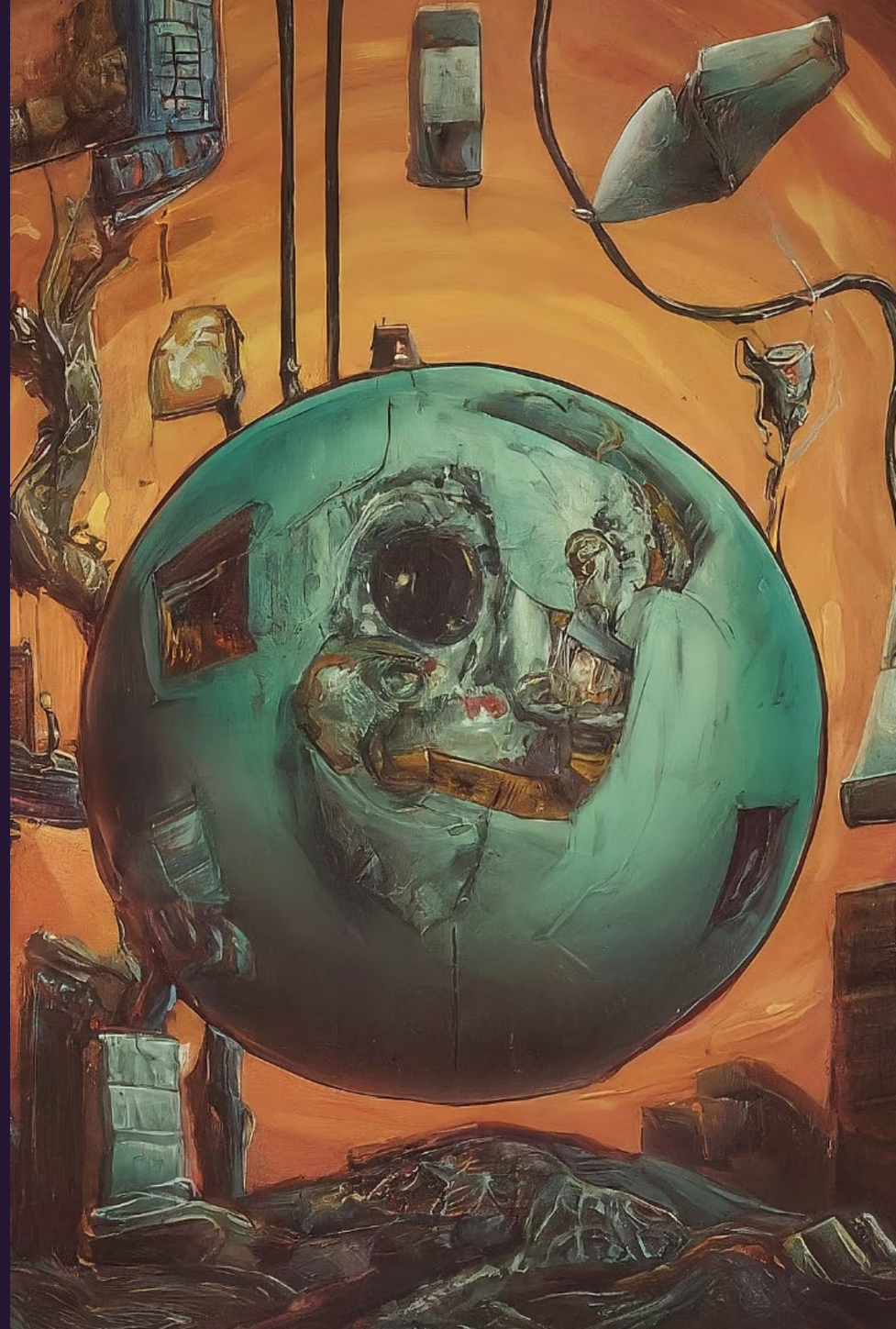
Пяскорская Екатерина Брониславовна

Индекс цифровой безопасности социокультурной среды

ФГБОУ ВО «СПБГУ» (Санкт-Петербург)

Актуальность изучения цифровой безопасности социокультурной среды

Современное общество все больше переходит в цифровую среду, что несет с собой как большие возможности, так и новые угрозы безопасности. Понимание и решение проблем цифровой безопасности социокультурной среды становится критически важной задачей для обеспечения защиты личных данных, снижения рисков киберпреступности и поддержания доверия граждан к цифровым технологиям.



Нормативно-правовое регулирование цифровых отношений в социокультурной сфере Российской Федерации

Указ президента РФ 2012-го года о мероприятиях по реализации государственной социальной политики

Исходя из этого указа не менее 10% издаваемых на территории российской федерации книг должны передаваться в электронные библиотеки, и музеи, и театры.

Федеральный закон "Об информации, информационных технологиях и о защите информации"

Этот закон устанавливает основные принципы и правила регулирования цифровых отношений в России, включая вопросы доступа, обработки и защиты данных.

Национальная программа "Цифровая экономика"

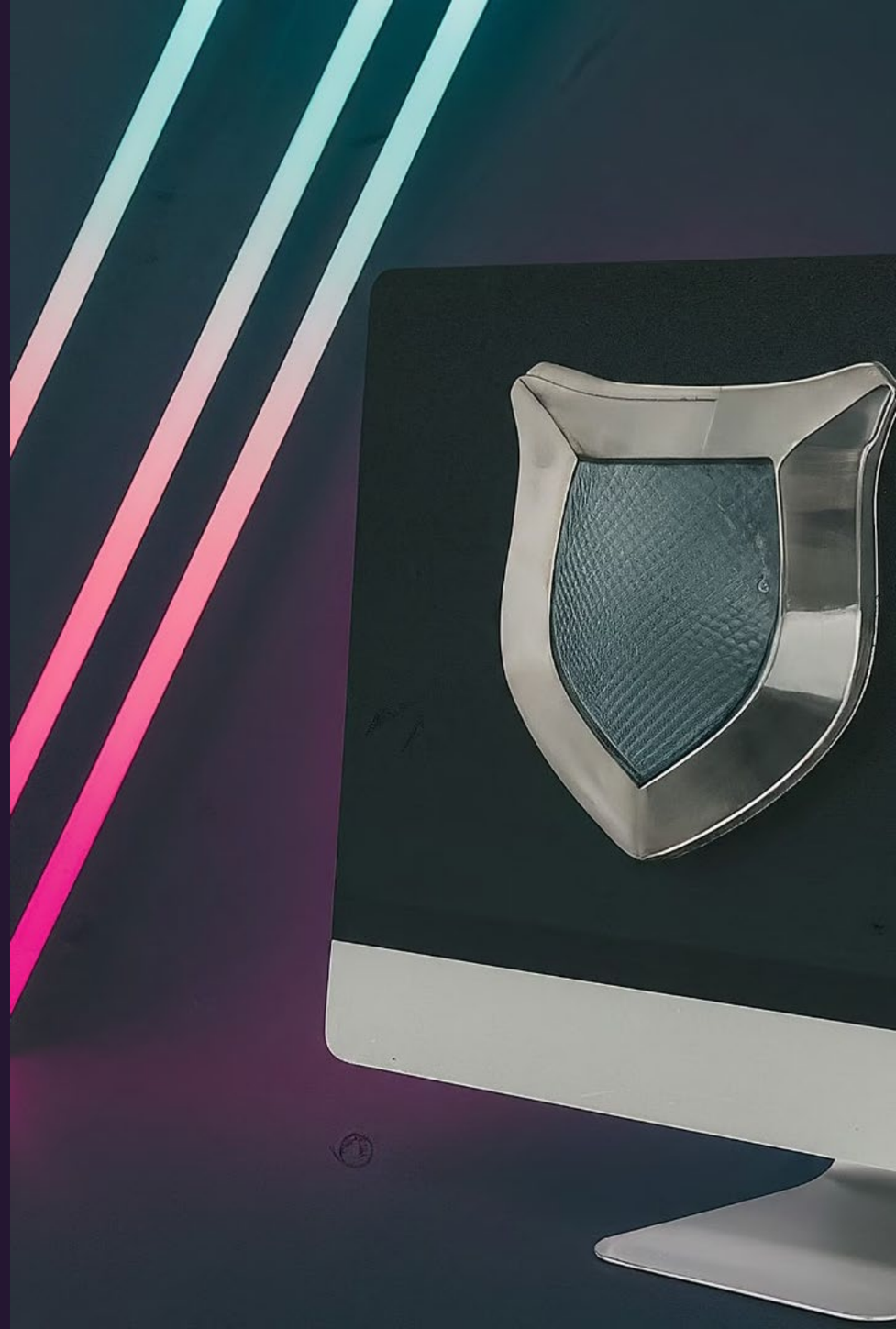
Программа нацелена на внедрение цифровых технологий во все отрасли экономики, в том числе в социокультурную сферу.

Национальный проект “Культура”

Помогает гражданам со всех уголков нашей страны реализовывать свои проекты, участвовать в социокультурной жизни своего города, помогая другим проектам.

Определение информационной безопасности

Информационную безопасность в данном случае необходимо рассматривать как открытую динамическую социальную систему, которая имеет свои специфические структурные и функциональные компоненты, так и общие с другими социальными системами черты. В качестве объектов системы выделяется следующие цели системы, которые отражают потребности личности общества: информационные интересы социальных объектов, как совокупность осознанных потребностей, совокупность основных социальных ценностей, силу обеспечения безопасности, субъекты обеспечения информационной безопасности, объекты информационной безопасности и ресурсы информационной безопасности.



Угрозы цифрового искусства, созданные на арт-рынках

1

Подделки и фальсификации

Электронные средства позволяют мошенникам создавать высококачественные подделки произведений искусства, которые трудно отличить от оригинала. Это подрывает доверие к цифровому арт-рынку.

2

Незаконное распространение

Интернет облегчает незаконное распространение и кражу цифровых произведений искусства. Это лишает художников и галереи законных доходов и ставит под угрозу целостность цифровой арт-экосистемы.

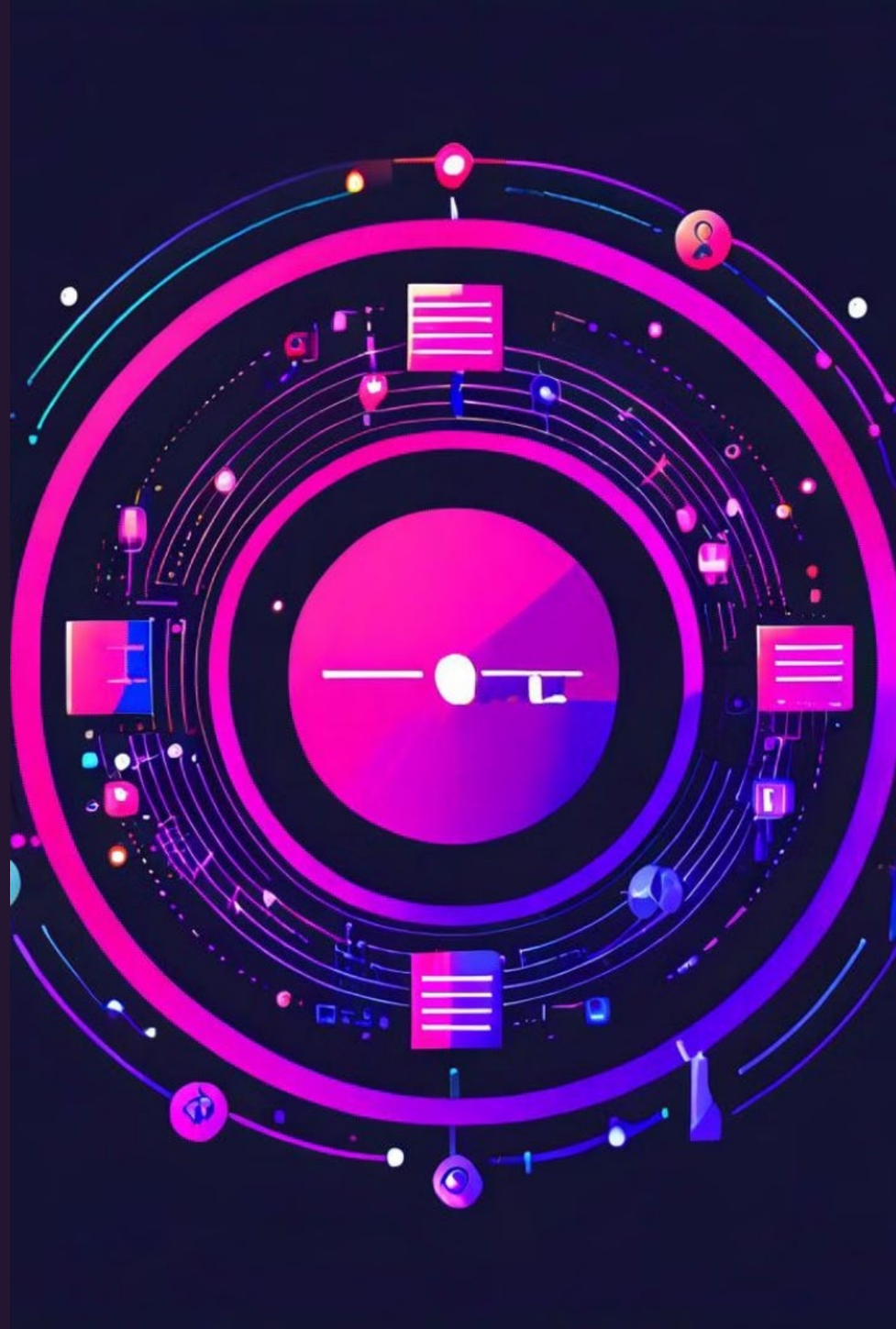
3

Манипуляции с ценами

Манипулирование ценами посредством роботов и алгоритмов создает нестабильность на цифровом арт-рынке. Это подрывает прозрачность и честность рынка.

Индекс цифровой безопасности социокультурной сферы

Индекс цифровой безопасности социокультурной сферы включает в себя ряд критериев, которые отражают различные аспекты информационной безопасности в цифровых технологиях, применяемых в области культуры и искусства. Этот индекс позволяет оценить уровень защищенности данных, конфиденциальность личной информации посетителей, а также уязвимости в системах безопасности онлайн-платформ.



Три свойства информационной безопасности

1. **Целостность:** Гарантия того, что информация и системы не были изменены или уничтожены несанкционированным образом. Это обеспечивает достоверность данных и работоспособность информационных систем.
2. **Доступность:** Своевременный и надежный доступ к информации и ресурсам для авторизованных пользователей. Это позволяет обеспечить непрерывность бизнес-процессов и предоставление услуг.

3. **Конфиденциальность:** Защита от несанкционированного раскрытия или доступа к информации. Гарантирует, что данные становятся доступны только тем, кому это разрешено.

Глобальном индексе кибербезопасности (GCI) на 2021-ый год РФ

В 2021 году Российская Федерация заняла 5-е место в Глобальном индексе кибербезопасности (GCI), который является международным стандартом для оценки готовности стран к противодействию киберугрозам. Этот рейтинг оценивает уровень национальных усилий в области кибербезопасности по пяти основным направлениям: законодательство, техническая оснащенность, организационные меры, потенциал и сотрудничество.

Вывод

- необходимо создать программы по повышению уровня цифровой грамотности населения, чтобы каждый мог защитить себя или обратиться за помощью к квалифицированным специалистам, которые помогут быстро разрешить проблему и раскрыть киберпреступление

- на государственном уровне принять единую концепцию борьбы с кибертерроризмом