# МЕТОДЫ И МОДЕЛИ ЭФФЕКТИВНОГО УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННЫХ СИСТЕМ

**Немчанинова С.В., Минзов А.С.**[1]

Государственный университет «Дубна», 141982, Московская обл., Дубна, ул. Университетская, 19, +79175156807, sbobylova94@gmail.com

[1]Государственный университет «Дубна», 141982, Московская обл., Дубна, ул. Университетская, 19, +79265650570, 926-565-0570@mail.ru

Активное внедрение информационных технологий во все сферы деятельности нашего общества и реализация национальной программы цифровой экономики привело к значительному росту числа информационных систем.

Практический опыт применения различных информационных систем показал, что далеко не всегда они используются эффективно, подвержены различного рискам со стороны внутренней и внешней среды функционирования, отказам технических и программных средств и уязвимостью их к киберугрозам. Последствия реализации этих рисков для государства и общества могут быть значительными, особенно это касается ИС управления критическими информационными инфраструктурами и социально значимыми объектами [1]. Отсюда и возникает необходимость исследования методов и технологий управления наиболее важными рисками для повышения эффективности функционирования этих ИС.

Понятие «непрерывность бизнеса» (business continuity) рассматривается как «стратегическая и тактическая способность организации планировать свою работу в случае инцидентов и нарушения ее деятельности, направленной на обеспечение непрерывности деловых операций на установленном приемлемом уровне» [2]. Общие подходы к созданию системы обеспечения непрерывности функционирования ИС были изложены в нормативном документе [3]. Стандарт построен на основе известных практик и выполнен форме рекомендаций. Такой подход не позволяет детализировать отдельные вопросы, связанные с конкретным выбором мер защиты, восстановления, управления и контроля состояния ИКТ. Ещё одна особенность этого стандарта заключается в том, что он распространяется и на системы менеджмента информационной безопасности. В стандарте реализован риск-ориентированный подход для определения приоритетов инцидентов, однако используемая методология рисков решает только одну задачу, установить приоритеты рисков на основе достаточно грубых классификаций в форме лингвистических переменных. Применение механизмов нечетких множеств не обеспечивает доверия к результатам, так как полученные значения параметров риска нельзя ни с чем сравнить и нет методов оценки их погрешности. Это не позволяет решать задачи, связанные с оценкой эффективности риск – ориентированных методов восстановления ИКТ и их оптимизации.

Таким образом, существующий уровень методического обеспечения непрерывности функционирования информационных систем не позволяет автоматизировать эти процессы из-за отсутствия параметрических моделей управления информационными рисками и неопределенности исходных данных.

**Литература.**

1. *Постановление Правительства РФ от 29 декабря 2021 г. N 2531 "Об утверждении Правил ведения перечня отечественных социально значимых информационных ресурсов".*
2. *ГОСТ Р 53647.22009: Менеджмент непрерывности бизнеса*
3. *ГОСТ Р ИСО/МЭК 27031-2012. Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса.*