УДК 004.056.

РАЗРАБОТКА МЕТОДИКИ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ КРЕДИТНО-ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

Тетерина А.В. (ИТМО)

Научный руководитель - кандидат технических наук, доцент Попов И.Ю. (ИТМО)

Введение. Для современных кредитно-финансовых организаций оценка рисков информационной безопасности представляет собой необходимый и непрерывный процесс, поскольку регулятором данного сектора в нашей стране является Банк России, который в свою очередь разработал стандарт ГОСТ Р 57580.1-2017[1]. Данный стандарт помимо всего прочего содержит требования к системе управления рисками в кредитно-финансовых организациях. Значительное внимание в документе уделяется операционному риску, коим и является риск информационной безопасности [2]. Исследование путей оптимизации оценки рисков информационной безопасности является актуальным, поскольку на государственном уровне не определена конкретная методика (за исключением субъектов критической информационной инфраструктуры) и на поддержание данного процесса ежегодно организации тратят большое количество человеко-часов,

Основная часть. Оценка рисков информационной безопасности – это процесс идентификации, анализа, оценки рисков информационной безопасности и реализация мер по управлению этими рисками [2]. Важным аспектом оценки рисков является определение их вероятности. Это позволяет более точно оценить степень уязвимости системы информационной безопасности и разработать соответствующие меры по управлению и митигации рисков. Для этого применяются различные методы, например, статистические методы, экспертные оценки, математическое моделирование и т.д. На сегодняшний день требования к оценке рисков информационной безопасности предъявляют такие стандарты: ISO 27001, PCI DSS, ГОСТ Р 57580.1. Также существует множество методик оценки рисков информационной безопасности, однако они редко учитывают реальные потребности бизнеса и те трудозатраты, которые он готов выделять на такой важный процесс ежегодно.

Выводы. Рассмотрены существующие методики оценки рисков информационной безопасности, проведён анализ нормативно-правовой базы, связанной с управлением рисками и разработана методика оценки рисков информационной безопасности для кредитно-финансовых организаций.

Список использованных источников:

1. Беляев Е.А., Емельянова О.А., Лившиц И.И. Анализ методик оценки рисков информационной безопасности кредитно-финансовых организаций // Научно-технический вестник информационных технологий, механики и оптики. – 2021. – С. 437-441.
2. Международный стандарт ISO/IEC 27005:2022. Информационная технология – Методы защиты – Менеджмент рисков информационной безопасности. – 2022.

[1] ГОСТ Р 57580.1-2017 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер. Введен 01.01.2018. М.: Стандартинформ, 2020. – 66 с