

УДК 004.05

**УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ
УПРАВЛЕНИЯ ОПЕРАЦИОННЫМИ РИСКАМИ КРЕДИТНЫХ ОРГАНИЗАЦИЙ
СОГЛАСНО ТРЕБОВАНИЯМ БАНКА РОССИИ**

Беляев Е.А. (федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»),

Научный руководитель – доктор технических наук Лившиц И.И.

(федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

Международными и государственными нормативными актами определено требование к управлению рисками информационной безопасности в кредитно-финансовых организациях. В январе 2022 года вступили в силу требования Положения Банка России от 08.04.2020 г. № 716-П, которым определены подходы в том числе к управлению рисками информационной безопасности в системе управления операционным риском, которые необходимы к выполнению в кредитных организациях.

Введение. Федеральными законами, международными и государственными стандартами, нормативными документами Банка России определено требование к управлению рисками информационной безопасности. Положением Банка России от 08.04.2020 г. № 716-П также определен относительно новый для банковской системы Российской Федерации термин «Операционный риск». Важность нового положения заключается в необходимости формирования банками отдельного капитала на покрытие вероятного ущерба от реализации операционного риска. В работе проведен анализ требований по управлению рисками информационной безопасности в системе операционных рисков.

Основная часть. Положением Банка России от 08.04.2020 г. №716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе» в системе управления операционным риском особое внимание уделено управлению риском информационной безопасности и риском информационных систем. Банк России ввел требования о необходимости в осуществлении в кредитных организациях различных оценок по информационной безопасности. Определена необходимость проведения мероприятий по тестированию на проникновение и проведение анализа уязвимостей объектов информационной инфраструктуры, оценка соответствия уровня защиты информации в отношении объектов информационной инфраструктуры кредитной организации, проводимая независимыми экспертами, оценка качества данных, тестирование уязвимостей информационных систем и (или) их компонентов и других источников рисков информационных систем. В работе предложены подходы к выполнению Положения в части сбора данных, классификации и мониторинга операционного риска, что необходимо для возможности расчета размеров операционного риска, включаемого в нормативы достаточности капитала кредитной организации, предложены способы автоматизации и оптимизации.

Выводы. В работе рассмотрен процесс управления риском информационной безопасности в системе управления операционным риском с учетом Положения Банка России от 08.04.2020 г. №716-П, которое определило и структурировало требования к кредитным организациям в части управления рисками информационной безопасности и информационных систем в системе операционного риска, в том числе риска, порядок учета рисков событий. Определены требования к разработке операционных систем, в том числе с учетом их влияния на обеспечение бесперебойной работы процессов кредитной организации, а также требования к отчетности. В работе предложены способы повышения эффективности внедрения системы операционным риском в кредитных организациях.

Беляев Е.А. (автор)

Лившиц И.И. (научный руководитель)