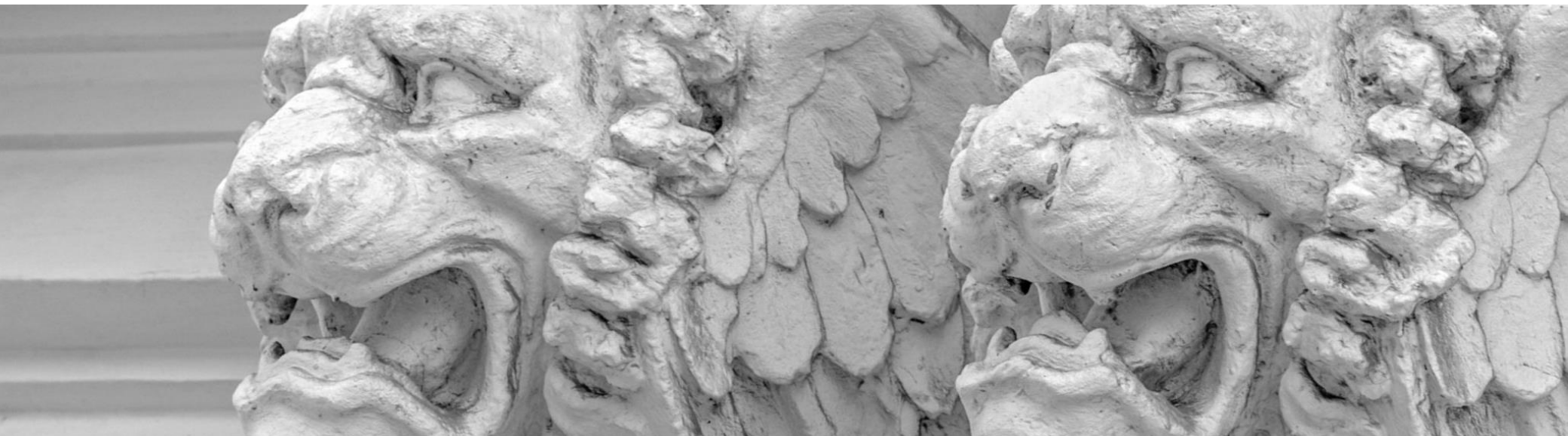




Банк России

Центральный банк Российской Федерации



Стандартизация в области обеспечения информационной безопасности некредитных финансовых операций

**Восьмой уральский форум
«Информационная безопасность
финансовой сферы»**
Республика Башкортостан
16-20 февраля 2016 года

Выборнов Андрей Олегович
начальник отдела методологии обеспечения безопасности
информационных ресурсов
Управления безопасности банковских информационных
банковских технологий
Главного управления безопасности и защиты информации
Банка России



Разработка отраслевых стандартов Банка России обеспечение информационной безопасности некредитных финансовых операций Российской Федерации

Развитие применения комплекса стандартов Банка России в связи с вступлением в силу Федерального закона от 27 июня 2011 г. N 162-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "О национальной платежной системе"



• Разработаны проекты стандартов:

Обеспечение информационной безопасности некредитных финансовых организаций. Общие положения (СТО БР ИБНФО Б-1.0)

Обеспечение информационной безопасности некредитных финансовых организаций, соответствующих критериям отнесения к малым предприятиям и микропредприятиям (СТО БР ИБНФО М-1.0)

• Разработка указанных проектов стандартов осуществлялась на основе Стандарта Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (СТО БР ИББС-1.0-2014)

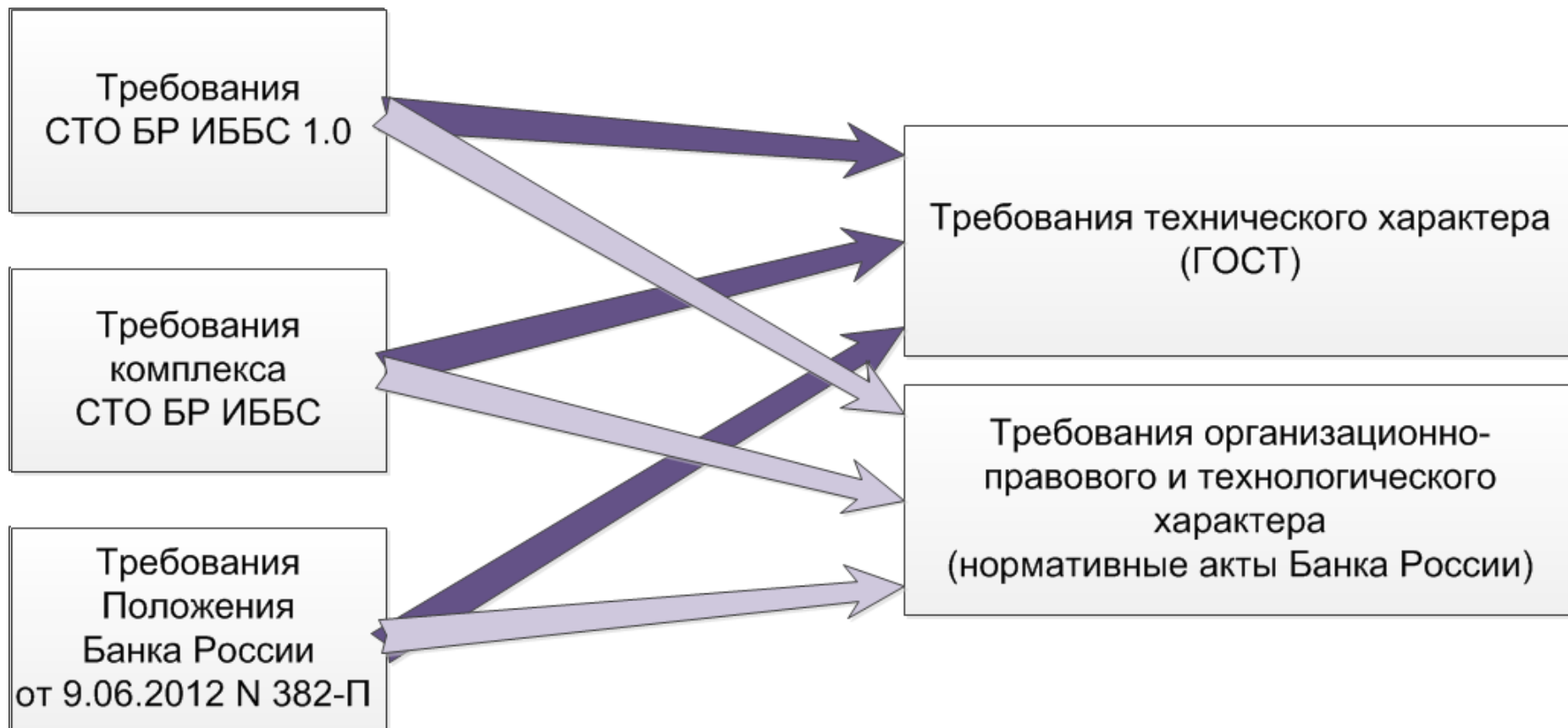
• Организована работа по согласованию проектов стандартов

• Основное содержание проектов стандартов

СТО БР ИБНФО Б-1.0	СТО БР ИБНФО М-1.0
Модели угроз и нарушителей информационной безопасности некредитных финансовых организаций Российской Федерации	Модели угроз и нарушителей информационной безопасности некредитных финансовых организаций Российской Федерации, соответствующих критериям отнесения к малым предприятиям и микропредприятиям
Система информационной безопасности. Общие требования...	
по обеспечению информационной безопасности при назначении и распределении ролей и обеспечении доверия к персоналу	
по обеспечению информационной безопасности автоматизированных систем на стадиях жизненного цикла	
по обеспечению информационной безопасности при управлении доступом и регистрацией	
по обеспечению информационной безопасности средствами антивирусной защиты	
по обеспечению информационной безопасности при использовании ресурсов сети Интернет	
по обеспечению информационной безопасности при использовании средств криптографической защиты информации	
по обеспечению информационной безопасности информационных технологических процессов	
по обработке персональных данных в некредитной финансовой организации Российской Федерации	по обработке персональных данных в некредитных финансовых организациях Российской Федерации, соответствующих критериям отнесения к малым предприятиям и микропредприятиям
по обеспечению информационной безопасности технологических процессов, в рамках которых обрабатываются персональные данные	



СТО БР ИБНФО Б-1.0	СТО БР ИБНФО М-1.0
Система менеджмента информационной безопасности. Требования к...	
организации и функционированию службы информационной безопасности некредитных финансовых организации Российской Федерации	координации деятельности связанной с информационной безопасностью
определению/коррекции области действия системы обеспечения информационной безопасности	
оценке и обработке рисков нарушения информационной безопасности при внедрении и (или) совершенствовании системы обеспечения информационной безопасности	внутренним документам, регламентирующим деятельность в области обеспечения информационной безопасности
разработке/коррекции внутренних документов, регламентирующих деятельность в области обеспечения информационной безопасности	разработке и организации реализации программ по обучению и повышению осведомленности в области информационной безопасности
реализации планов и решений по внедрению и (или) совершенствованию системы обеспечения информационной безопасности	
разработке и организации реализации программ по обучению и повышению осведомленности в области информационной безопасности	
организации обнаружения и реагирования на инциденты информационной безопасности	
организации информационной безопасности для обеспечения непрерывности бизнеса и его восстановления после прерываний	
мониторингу информационной безопасности и контролю защитных мер	
проведению самооценки и аудита информационной безопасности	проведению оценки соответствия (самооценки, независимой оценки - аудиту) информационной безопасности
анализу функционирования системы обеспечения информационной безопасности	
анализу системы обеспечения информационной безопасности со стороны руководства некредитных финансовых организации Российской Федерации	
принятию решений по тактическим улучшениям системы обеспечения информационной безопасности	
принятию решений по стратегическим улучшениям системы обеспечения информационной безопасности	

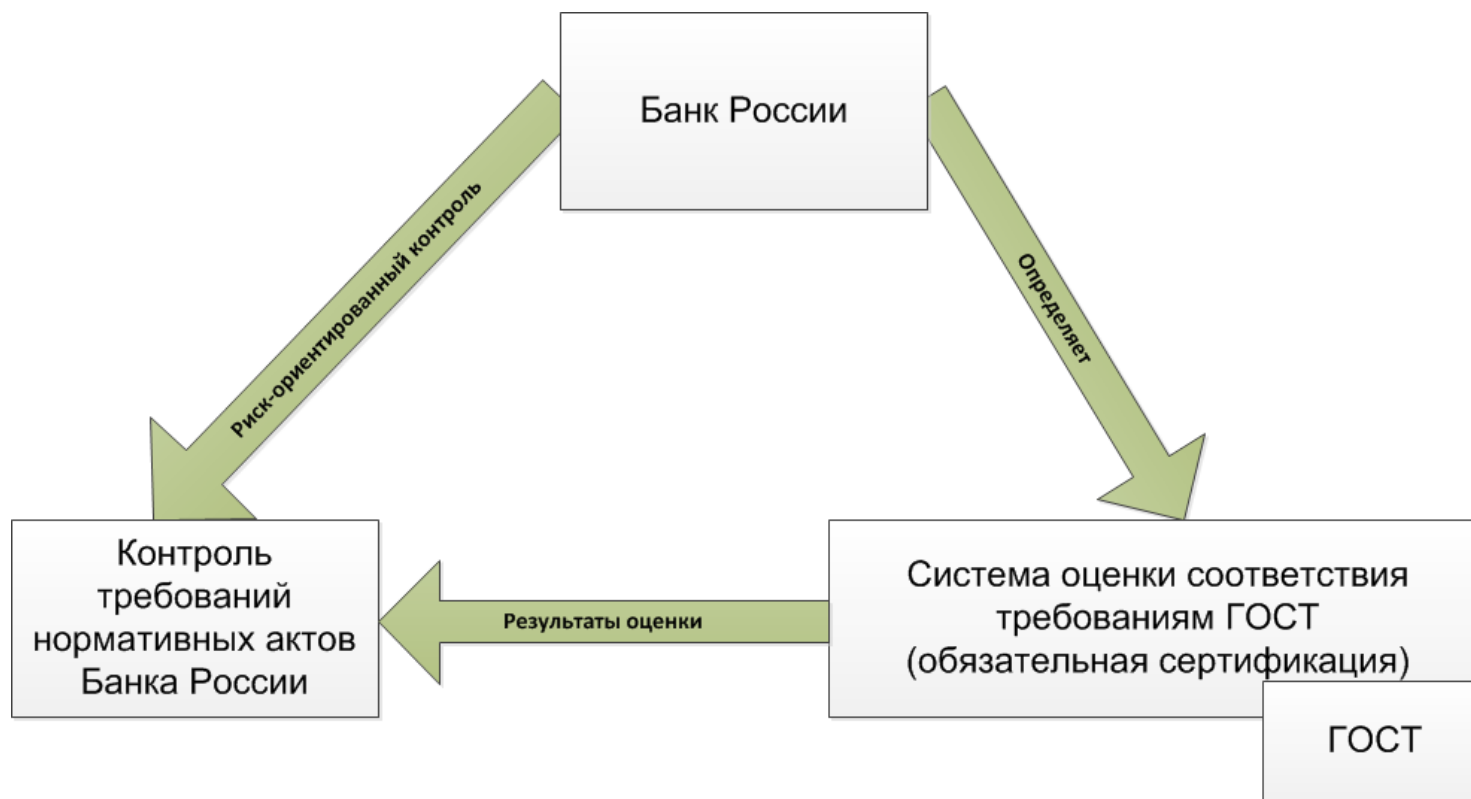




Исключение технических вопросов обеспечения информационной безопасности

Установление нормативных ссылок на ГОСТ (ГОСТ обязательны к применению)

Установление только технологических и организационных требований





ГОСТ регламентирует технические вопросы обеспечения информационной безопасности в КО и НФО

Работающая система оценки соответствия выполнения КО и НФО требований ГОСТ

Нормативные акты Банка России, устанавливающие только технологические и организационные требования и содержащие нормативные ссылки на требования ГОСТ

Контроль выполнения требований нормативных актов Банка России, учитывающий результаты оценки соответствия требованиям ГОСТ



Банк России

Центральный банк Российской Федерации



Благодарю за внимание!