Банк России

ИЗМЕНЕНИЯ В ГОСТ 57580.1, ГОСТ 57580.2. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПРОВЕДЕНИЮ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ И АНАЛИЗУ ЗАЩИЩЕННОСТИ

Стародубов К.В.
Департамент информационной безопасности

2024 г.

1 Изменения в ГОСТ 57580.1 и ГОСТ 57580.2

Рабочие группы
Цели и задачи
Изменения в ГОСТ 57580.1
Изменения в ГОСТ 57580.2
Дальнейшие планы

Необходимость изменений

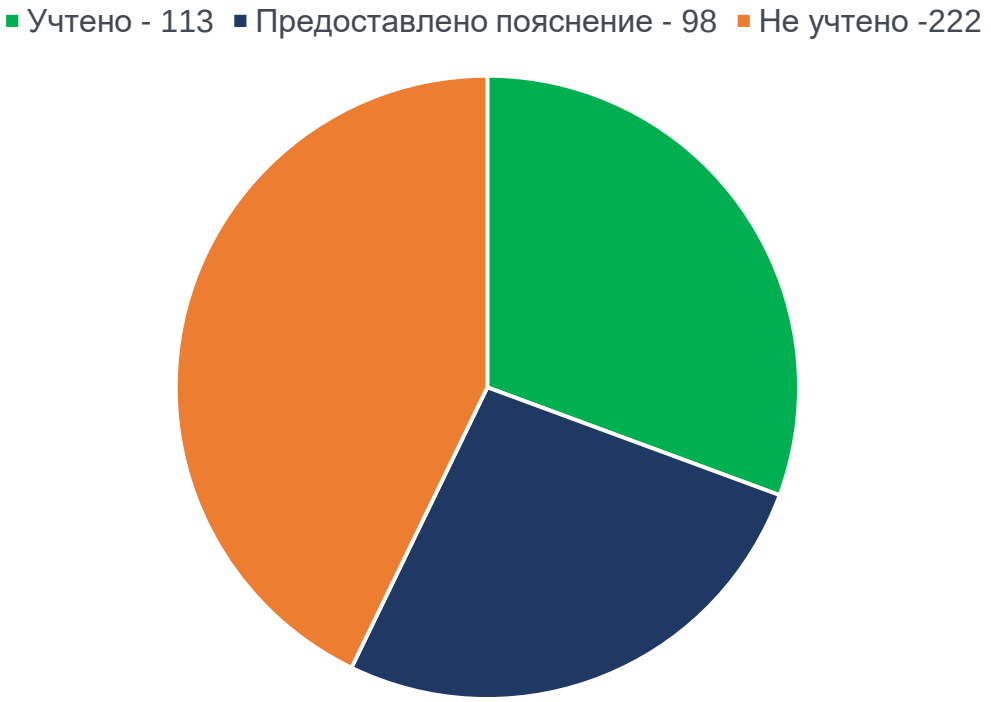
Департаментом информационной безопасности в связи с запросом представителей финансового рынка о необходимости совершенствования регулирования и стандартизации в областях защиты информации и операционной надежности, поступившим на последнем Уральском форуме «Кибербезопасность в финансах», создана рабочая группа:

Рабочая группа «**Ревизия положений** национальных стандартов Российской Федерации **ГОСТ Р 57580.1** «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» **и ГОСТ Р 57580.2** «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия» **(далее – РГ-1)**

Рабочая группа

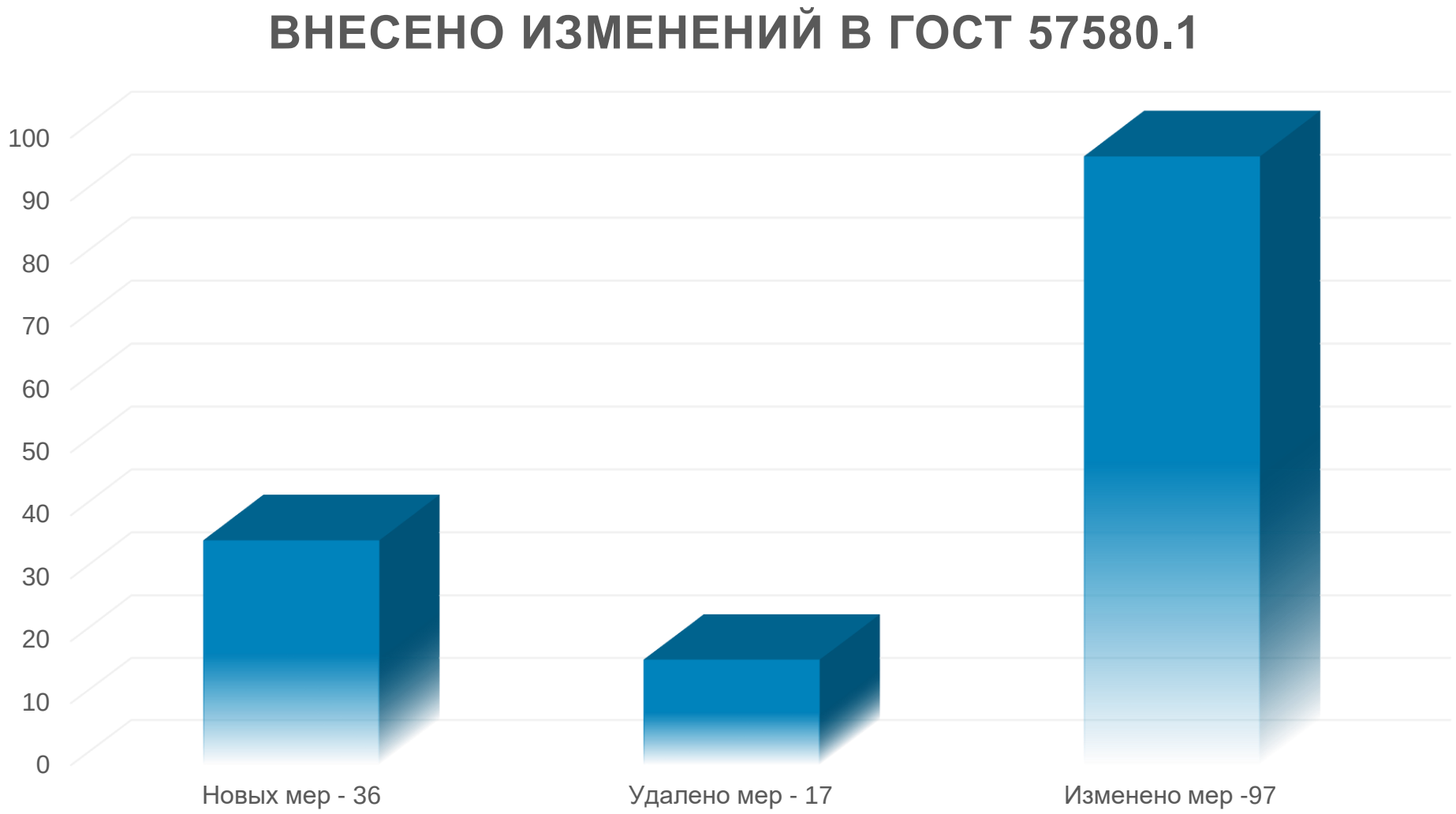
По РГ-1 на заочное голосование выносилось 196 предложений. На текущий момент по результатам заочного голосования и дополнительного рассмотрения учтено или частично учтено порядка 130.

Изменения в ГОСТ 57580.1
424 предложений поступило



Изменения в ГОСТ 57580.2
37 предложений поступило

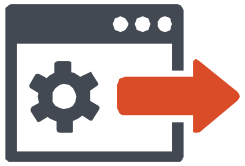
Основные изменения в ГОСТ 57580.1



Основные изменения в ГОСТ 57580.1

Расширен субъектный состав – Добавлены ЛОПУФРы, ФинТех организации и организации, осуществляющие деятельность на основании законодательства РФ

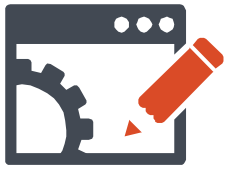
Переработан и синхронизирован Процесс 3 – «Контроль целостности и защищенности информационной инфраструктуры» – переработан и синхронизирован с нормативными документами ФСТЭК России по контролю уязвимостей.



Переработан Процесс 8 – «Защита информации при осуществлении удаленного доступа» – переработан с учетом удаленных рабочих мест.

Обновлены определения – Добавлены недостающие определения (например, мобильное устройство, МНИ и т.д.).

Переработан и разделен Процесс 7 – «Защита среды виртуализации и контейнеризации» – переработан и разделён на требования к виртуализации и контейнерам, добавлены новые меры по контейнерам.



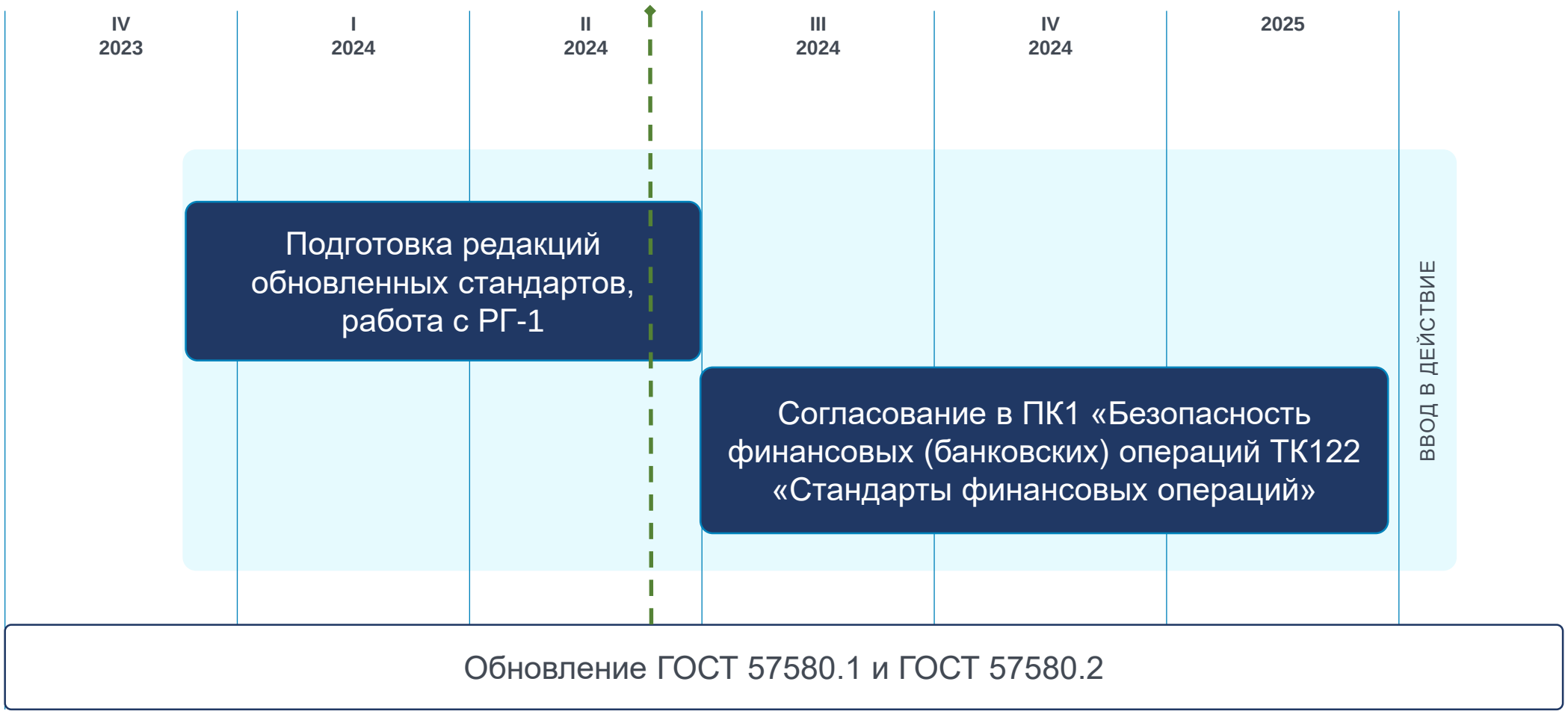
Приведено в соответствие Приложение Б – «Состав и содержание организационных мер, связанных с обработкой финансовой организацией персональных данных» - приведено в соответствие с нормативными документами по защите ПДн.

Основные изменения по ГОСТ Р 57580.2 :

Уточнен критерий «независимости» – проверяющей организации по отношению к проверяемой, оптимизирован подход по оформлению перечня свидетельств, добавлена формула для расчета оценки соответствия для нескольких контуров безопасности с одинаковым уровнем защиты информации.

Убрана подпись –
В формах листов для сбора свидетельств оценки соответствия ЗИ убрана подпись члена (членов) проверяющей группы и сотрудника (сотрудников) проверяемой организации, при этом добавлена форма итоговой подписи всех членов проверяемой группы. Добавлены дополнительные требования к отчету по результатам оценки соответствия ЗИ (пункт 8.4 ГОСТ)

Дальнейшие планы



2 Тестирование на проникновение и анализ уязвимостей

Разработка МР Банком России
Цели и задачи
Содержание МР
Дальнейшие планы

Разработка МР Банком России

Согласовано АФТ

В целях обеспечения единого подхода к реализации требований по проведению тестирования на проникновение и анализа уязвимостей информационной безопасности

Организации финансового рынка:

- кредитные организации
- некредитные финансовые организации
- субъекты национальной платежной системы
- лица, оказывающие профессиональные услуги на финансовом рынке

Положения Банка России:

- № 683-П
- № 757-П
- № 821-П
- № 808-П

Объекты информационной инфраструктуры:

- автоматизированные системы
- программное обеспечение
- средства вычислительной техники
- телекоммуникационное оборудование

Цели и задачи

ПОДХОД К ТЕСТИРОВАНИЮ

Цели

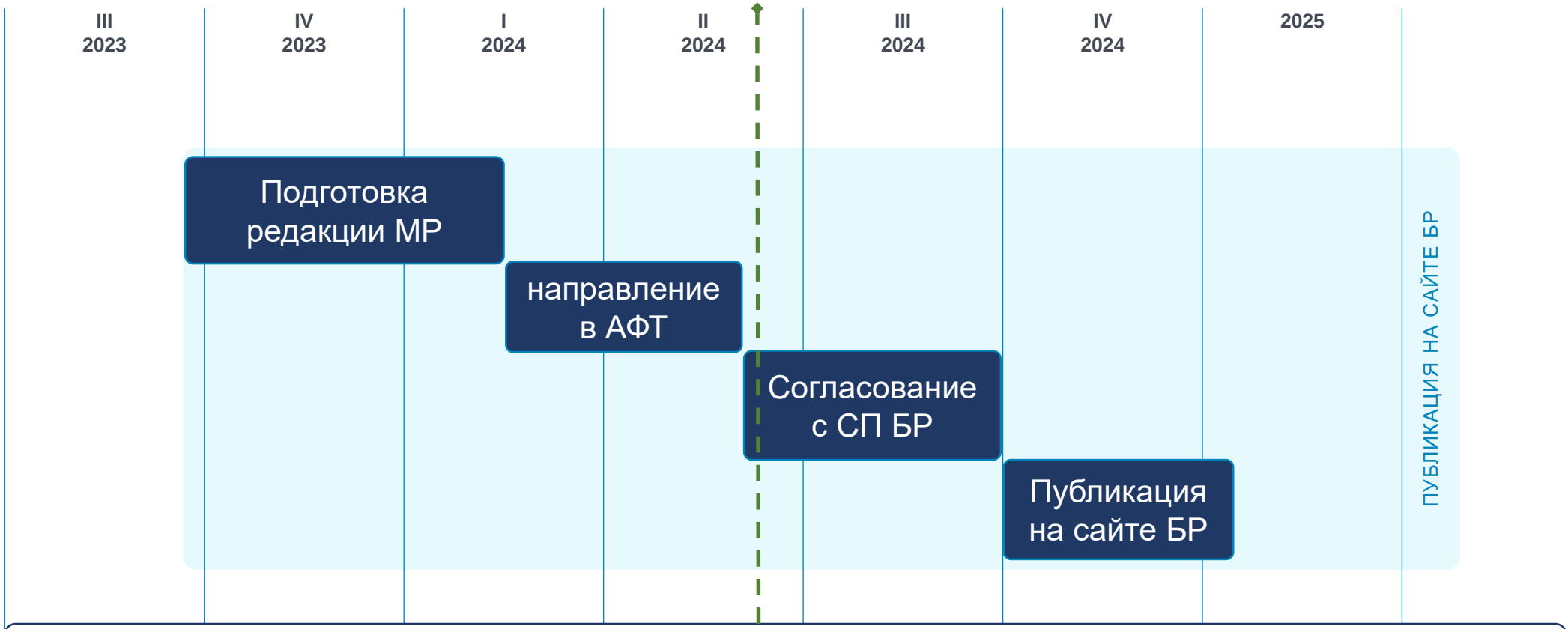
- оценка уровня защищенности объектов информационной инфраструктуры организации финансового рынка;
- обеспечение доверия к объектам информационной инфраструктуры, в том числе входящим в критичную архитектуру.

Задачи

- выявление уязвимостей, определение способов эксплуатации уязвимостей или нарушения функций безопасности объектов информационной инфраструктуры организации финансового рынка, которые могут привести к возникновению негативных последствий нарушения информационной безопасности, в том числе потерь организации финансового рынка, ее клиентов и контрагентов;
- разработка рекомендаций по устранению уязвимостей информационной безопасности;
- идентификация риска информационной безопасности (в том числе выявления нарушений (риска нарушения) требований к обеспечению защиты защищаемой информации или обеспечению операционной надежности), включая случаи, когда реализация такого риска приводит к совершению операций без согласия клиента, а также описание его влияния на общую защищенность и формирование рекомендаций по минимизации риска.

Содержание

Дальнейшие планы



Разработка проекта Методических рекомендаций по проведению тестирования на проникновение и анализу уязвимостей информационной безопасности объектов информационной инфраструктуры организаций финансового рынка

Банк России

СПАСИБО ЗА ВНИМАНИЕ

starodubovkv@cbr.ru

2024 г.