ФБК
Аудит | Консалтинг | Право

Новые стандарты 57580.3-2022 и 57580.4-2022 для финансовых организаций: анализ и алгоритм пошагового внедрения

Михаил Манцуров
Старший консультант по ИТ, ФБК

Устойчивое развитие финансовой отрасли в РФ все больше зависит от того, как она управляет используемыми информационными технологиями и противодействует информационным угрозам

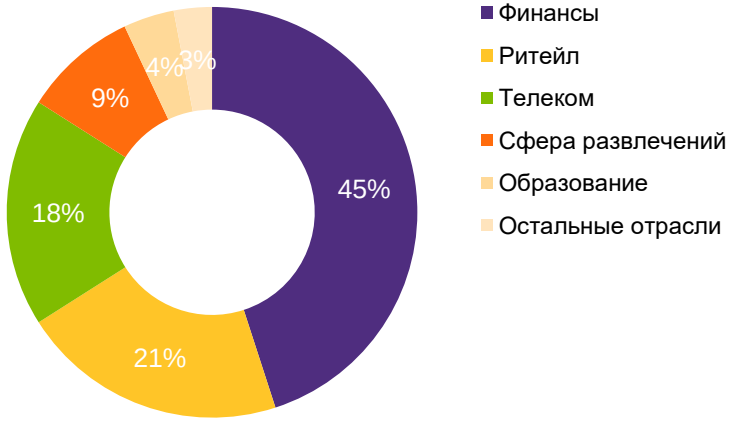
Информационные угрозы для финансового сектора

- рост числа кибератак
- уход с рынка иностранных поставщиков оборудования и программного обеспечения
- вопросы импортозамещения и технологического суверенитета
- атаки кибермошенников на деньги граждан
- переход на дистанционную работу

В 2022 году объем операций без согласия клиентов на фоне развития дистанционных платежных сервисов увеличился по сравнению с 2021 годом на 4,29% и составил **14 165,44 млн руб**.

Source: https://www.cbr.ru/analytics/ib/operations_survey_2022/

DDoS-атаки в России в 2022 году



> Количество DDoS-атак на финансовые организации в России в минувшем году выросло в четыре раза, общее число киберугроз увеличилось на 2%

зампред Банка России Филипп Габуния на форуме «Кибербезопасность в финансах-2023»

Source: https://stormwall.pro/, https://www.interfax.ru/russia/886331

Вопросы противодействия информационным угрозам и киберустойчивости в регуляторном фокусе Банка России

2018 — Введение **ГОСТ Р 57580.1-2017** по защите информации финансовых организаций и **ГОСТ Р 57580.2-2018** по оценке соответствия

2019 — Нормативные ссылки на ГОСТ Р 57580.1-2017 и ГОСТ Р 57580.2-2018 (**требования об обязательности исполнения**) появляются в нормативных актах Банка России (№ 672-П, № 683-П, № 684-П)

2022 — Продолжение разработки ГОСТ в области информационной безопасности и киберустойчивости **в рамках подкомитета №1 Технического комитета №122 Росстандарта**

2023 — **Введение ГОСТ Р 57580.3-2022 и ГОСТ Р 57580.4-2022** по управлению риском реализации информационных угроз и обеспечению операционной надежности

В разработке Подкомитета №1 Технического комитета №122 **находятся проекты стандартов с оценкой зрелости (для ГОСТ Р 57580.3) и оценкой соответствия (для ГОСТ Р 57580.4)**

2024? — **Включение нормативных ссылок на новые стандарты в акты Банка России – вопрос ближайшего времени**

Структура комплекса стандартов серии 57580

Комплекс национальных стандартов «Безопасность финансовых (банковских) операций»

Семейство стандартов управления риском (УР)	Управление риском реализации информационных угроз и обеспечение операционной надежности
	Методика оценки зрелости
Семейство стандартов операционной надежности (ОН)	Обеспечение операционной надежности
	Методика оценки соответствия
Семейство стандартов защиты информации (ЗИ)	Защита информации финансовых организаций
	Методика оценки соответствия

Специфика стандартов

ГОСТ Р 57580.3-2022

- базовый в рамках всего комплекса стандартов серии
- задает общую терминологию, цели и состав требований по управлению риском реализации информационных угроз и обеспечению операционной надежности
- регламентирует порядок управления риском реализации информационных угроз

ГОСТ Р 57580.4-2022

- регламентирует порядок управления системой обеспечения операционной надежности
- является детальным руководством по исполнению требований к операционной надежности, установленных №787-П и №779-П)

Заложенные подходы

- принцип пропорционального регулирования: меры (О, Т, Н) для каждого уровня защиты информации
- создание систем управления: PDCA (Plan – Do – Check – Act)
- интегрирование в систему управления операционным риском
- объект применения – критичная архитектура в разрезе бизнес- и технологических процессов
- риск-ориентированный подход при реализации

Проблемы реализации

- большой объем стандартов, сложность восприятия
- учет специфики деятельности организации и применение риск-ориентированного подхода
- разработка большого количества внутренней документации
- большое количество подлежащих идентификации, учету и контролю элементов критичной архитектуры
- необходимость привлечения ресурсов (кадровых, временных, финансовых, технологических)
- необходимость вовлечения руководства
- сложность в распределении ролей и границ ответственности
- необходимость выстраивания эффективной (и оперативной) коммуникации и вовлечения всего персонала

Алгоритм пошагового внедрения положений стандартов: практические рекомендации

Алгоритм пошагового внедрения стандартов

В рамках созданной рабочей группы по реализации стандартов (ИТ, ИБ, СУР, бизнес, внутренний аудит и контроль)

Основные шаги внедрения

1. Определение ролей и границ ответственности

- пересмотр функционала подразделений, представители которых входят в созданную рабочую группу
- координация работы должностным лицом, ответственным за функционирование системы управления риском реализации информационных угроз
- определение ролей руководства в процессах
- закрепление согласованных ролей во внутренних документах

2. Разработка внутренних нормативных документов

- разработка (доработка) основных ВНД по управлению риском реализации информационных угроз и обеспечению операционной надежности
- корректировка внутренних документов по управлению операционным риском

Основные шаги внедрения

3. Определение бизнес- и технологических процессов

- составление (сверка) перечня технологических процессов организации, а также связанных с ними бизнес процессов (см. Приложение В к ГОСТ Р 57580.3-2022)
- назначение владельцев процессов
- описание процесса, в том числе участники, характер и последовательность выполняемых процедур (текстовое, нотации BPMN или TOGAF)

4. Идентификация критичной архитектуры

- выделение объектов информатизации, задействованных в выполнении процессов (до конфигурации, например, в формате CPE:2.3)
- определение задействованных ИТ-поставщиков
- определение задействованного персонала
- фиксация результатов (Microsoft Excel, CMDB в ITSM-системе, Confluence, системы класса менеджмента ИТ-активов ITAM)

Основные шаги внедрения

5. Мониторинг операций и сбор статистики

- обеспечение мониторинга ИТ-инфраструктуры на предмет выявления проблем и сбоев (например, Zabbix)
- сбор бизнес-метрик (количество операций/посетителей, а также динамика операций в сравнении с предыдущими аналогичными периодами)

6. Разработка сценариев реализации информационных угроз

- идентификация, описание и оценка основных возможных ситуаций реализации информационных угроз, в том числе в части прерывания деятельности организации – применительно к критичной архитектуре
- определение для сценариев последовательности возможных действий и их источников (например, с использованием Методики оценки угроз от ФСТЭК или матрицы MITRE ATT&CK)
- встраивание разработки сценариев в процесс сценарного анализа операционного риска (при наличии)

Основные шаги внедрения

7. Установление контрольных и целевых показателей

- установление (сверка) контрольных и целевых показателей, предусмотренных стандартами, учитывая нормативные требования Банка России
- определение целевого времени восстановления (ЦВВ) и целевой точки восстановления данных (ЦТВД) в отношении процессов (обеспечивающих их выполнение ИС)

(использование для расчета показателей накопленной статистики операций, истории рисковых событий, лимитов, установленных Банком России, а также мотивированного мнения экспертов)

8. Управление изменениями в критичной архитектуре

- обеспечение планирования, оценки (в том числе на предмет существующих рисков), утверждения, реализации и последующего контроля изменений в критичной архитектуре
- использование имеющегося инструментария (например, системы Service Desk или внутреннего портала)

Основные шаги внедрения

9. Работа с персоналом и ИТ-поставщиками

- доведение до персонала информации о внедряемых мерах и об актуальных информационных угрозах (ознакомление с ВНД, справочные материалы, памятки, рассылки, обучение)
- пересмотр заключаемых в ИТ-поставщиками договоров (включение обязательств по ИБ, конфиденциальности, непрерывности оказания услуг)
- заключение (пересмотр) SLA с ключевыми поставщиками (с учетом установленных целевых показателей)

10. Регистрация инцидентов и периодическое тестирование

- обеспечение выявления, сбора, регистрации информации об ИБ-инцидентах и простоях, анализ причин и оценка потерь от них
- проведение периодического тестирования готовности организации противостоять информационным угрозам в отношении критичной архитектуры (например, рассылка фишинговых писем, восстановление из резервной копии, переход на резервную ИТ-инфраструктуру)

Основные шаги внедрения. Что нужно сделать еще

- обеспечение **эффективной коммуникации между подразделениями** на всех этапах
- доведение информации о **порядке действий в случае выявления инцидентов** (нежелательных событий) до персонала (с указанием контактных данных ответственных лиц)
- **аккумулирование данных и результатов работы в единой точке**

  (собранную информацию об элементах критичной архитектуры и процессах изменений в ней, состоянии ИТ-инфраструктуры, статистике операций, значениях контрольных и целевых показателей, инцидентах, каналах коммуникации необходимо аккумулировать в единой точке (на основе имеющихся средств автоматизации (Jira или иные средства совместной работы, внутренний портал, отдельные дашборды в одной из BI-систем))

Выводы

Предложенный пошаговый алгоритм

- позволяет начать внедрять отдельные положения стандартов **уже сейчас, не дожидаясь вступления в силу требований об их обязательности**
- учитывает приоритетность выполняемых мероприятий
- основан на использовании **существующих** в организации ресурсов и встраивании в **существующие** в организации процессы

Новые стандарты серии 57580

- несмотря на некоторую сложность, **аккумулируют в себе хорошие практики и опыт**
- могут быть полезны для многих организаций
- могут помочь навести и поддерживать порядок в ИТ-инфраструктуре
- могут повысить безопасность и обеспечить непрерывность оказания услуг клиентам (⟹ **повысить их доверие и лояльность**)

Постепенное и заблаговременное внедрение мер новых стандартов – наиболее оптимальный вариант

Контакты

Алексей Карпушкин
Руководитель направления по IT аудиту
Aleksey.Karpushkin@fbk.ru

Михаил Манцуров
Старший консультант по IT
Mikhail.Mantsurov@fbk.ru

ФБК

Аудит | Консалтинг | Право

Спасибо за внимание!

ул. Мясницкая, 44/1,
Москва, Россия 101990

T: (495) 737 5353
Ф: (495) 737 5347
E: fbk@fbk.ru

fbk.ru
fbk-pravo.ru
fbkcs.ru