ГОСТ 57580.3-2022 «УПРАВЛЕНИЕ РИСКОМ РЕАЛИЗАЦИИ ИНФОРМАЦИОННЫХ УГРОЗ И ОБЕСПЕЧЕНИЕ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ»

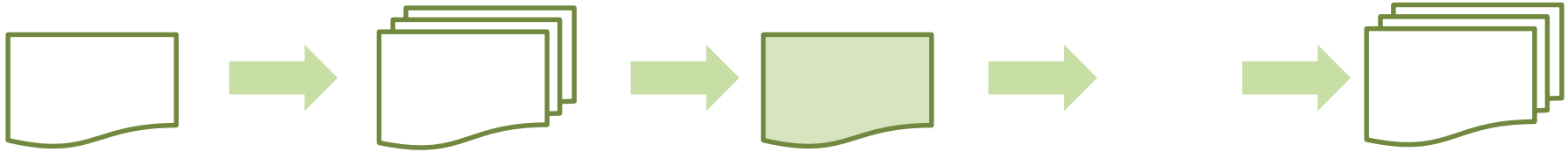
ТРЕБОВАНИЯ И ПОДХОДЫ К ИХ РЕАЛИЗАЦИИ

Антон Свинцицкий
Директор по консалтингу
АО «ДиалогНаука»

31 октября 2023 года, Москва

ДиалогНаука

Меры защиты и управление рисками ИБ



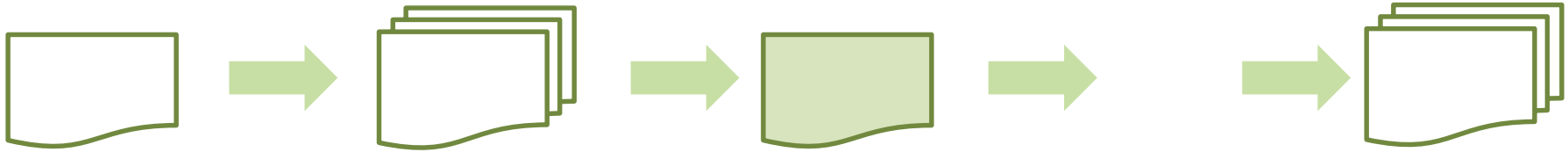
СТО БР ИББС 1.0-2004

СТО БР ИББС 1.0-2006
СТО БР ИББС 1.1-2007
СТО БР ИББС 1.2-2007

РС БР ИББС 2.2-2009

СТО БР ИББС 1.0-2014
СТО БР ИББС 1.4-2014

Меры защиты и управление рисками ИБ



СТО БР ИББС 1.0-2004

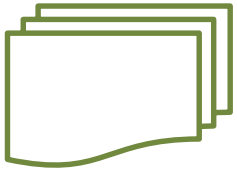
СТО БР ИББС 1.0-2006
СТО БР ИББС 1.1-2007
СТО БР ИББС 1.2-2007

РС БР ИББС 2.2-2009

СТО БР ИББС 1.0-2014
СТО БР ИББС 1.4-2014

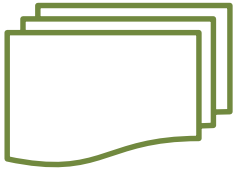
Меры защиты и управление рисками ИБ

СТО БР ИББС 1.0-2004

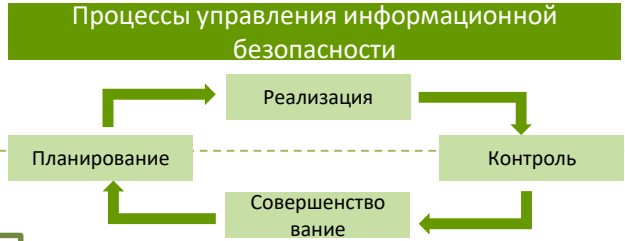


СТО БР ИББС 1.0-2006
СТО БР ИББС 1.1-2007
СТО БР ИББС 1.2-2007

РС БР ИББС 2.2-2009



СТО БР ИББС 1.0-2014
СТО БР ИББС 1.4-2014

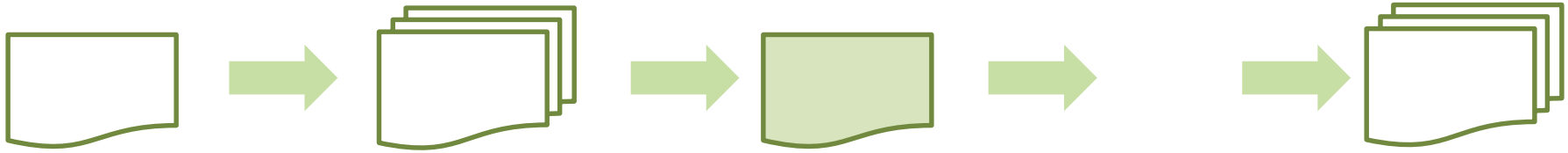


Положение БР 382-П
(от 2012 года)

Положения БР 683-П
Положения БР 802-П
Положения БР 719-П
Положения БР 757-П

ГОСТ Р 57580.1
ГОСТ Р 57580.2

Меры защиты и управление рисками ИБ

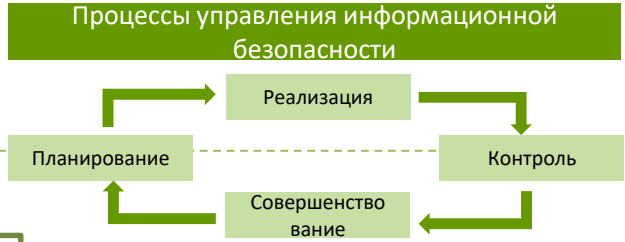


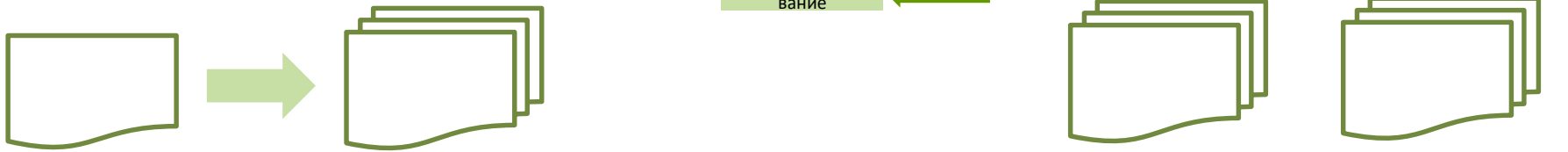
СТО БР ИББС 1.0-2004

СТО БР ИББС 1.0-2006
СТО БР ИББС 1.1-2007
СТО БР ИББС 1.2-2007

РС БР ИББС 2.2-2009

СТО БР ИББС 1.0-2014
СТО БР ИББС 1.4-2014





Положение БР 382-П
(от 2012 года)

Положения БР 683-П
Положения БР 802-П
Положения БР 719-П
Положения БР 757-П

ГОСТ Р 57580.1
ГОСТ Р 57580.2

ГОСТ Р 57580.3
ГОСТ Р 57580.4

Положения Банка России

Центральный банк Российской Федерации

787-П (779-П)

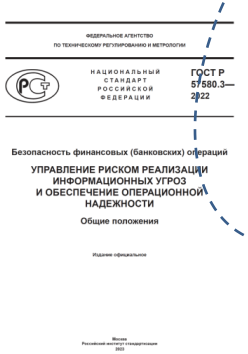
716-П

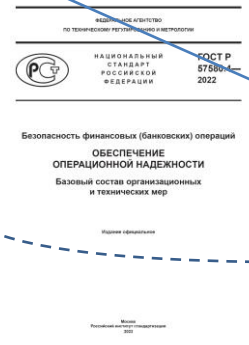
683-П

719-П

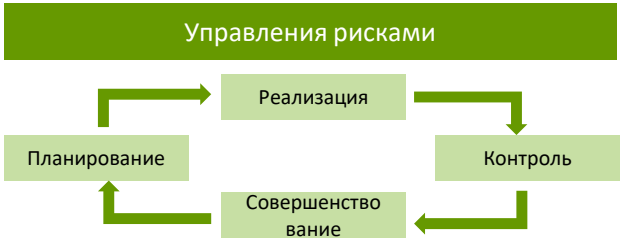
757-П

802-П





Положение Банка России 716-П и виды рисков



Виды операционного риска:

- ✓ Риск реализации угроз безопасности информации (риск ИБ)
- ✓ Риск отказов и(или) нарушения функционирования информационных систем (риск информационных систем)

Положение Банка России 716-П и виды рисков

Виды операционного риска:

- ✓ Риск реализации угроз безопасности информации (риск ИБ)
- ✓ Риск отказов и(или) нарушения функционирования информационных систем (риск информационных систем)

События операционного риска → ? → Несоответствие требованиям по защите информации → ? → Оценка негативного влияния (потери) → ?

- ✓ Приостановка и(или) прекращение банковских процессов
- ✓ Потеря работоспособности объектов информационной инфраструктуры

Риски ИБ и Риски информационных систем

Политика ИБ

Участие совета директоров

Политика ИС

Риски ИБ и Риски информационных систем

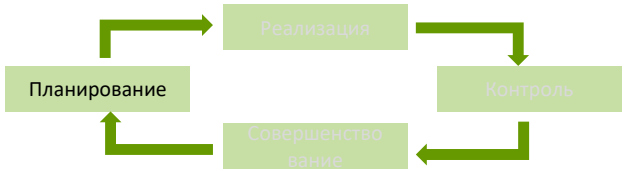
Политика ИБ

- ✓ Распределение зон ответственности
- ✓ Кадровые и финансовые ресурсы

Определение процесса управления рисками ИБ

Участие совета директоров

Управления рисками ИБ



Политика ИС

- ✓ Распределение зон ответственности (функции и полномочия)
- ✓ Требования к качеству
- ✓ Порядок взаимодействия
- ✓ Отчетность

Архитектура ИС

- ✓ Требования к структуре ИС
- ✓ Требования к стандартизации и унификации
- ✓ Требования к надежности функционирования
- ✓ Требования к качеству данных

Риски ИБ и Риски информационных систем

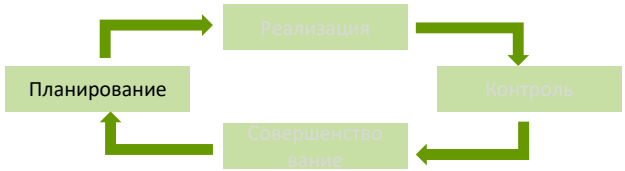
Политика ИБ

- ✓ Распределение зон ответственности
- ✓ Кадровые и финансовые ресурсы

Определение процесса управления рисками ИБ

Участие совета директоров

Управления рисками ИБ



Политика ИС

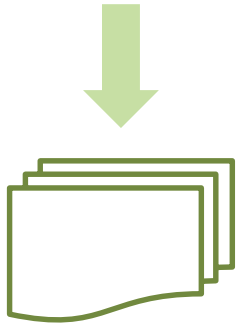
- ✓ Распределение зон ответственности (функции и полномочия)
- ✓ Требования к качеству
- ✓ Порядок взаимодействия
- ✓ Отчетность

Архитектура ИС

- ✓ **Требования к структуре ИС**
- ✓ **Требования к стандартизации и унификации**
- ✓ Требования к надежности функционирования
- ✓ Требования к качеству данных

Риски информационной безопасности

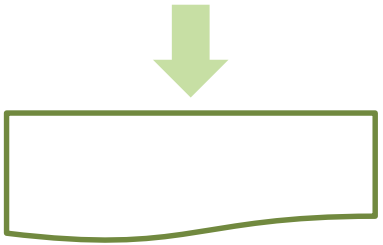
- ✓ Выявление событий риска
- ✓ Ведение базы событий риска ИБ
- ✓ Повышение осведомленности
- ✓ Выполнение требований НПА Банка России
- ✓ Защита от угроз



Отчетность на периодической основе

Риски ИБ и Риски информационных систем

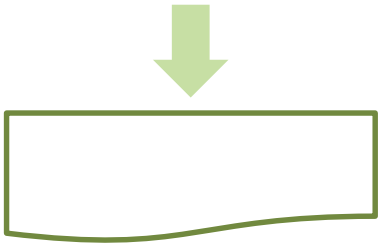
- ✓ Реализация программ контроля (программ аудита)
- ✓ Тестирование на проникновение
- ✓ Мониторинг рисков ИБ
- ✓ Контроль КПУР
- ✓ Независимая оценка на ежегодной основе (например, службой внутреннего аудита)



Отчетность на периодической основе

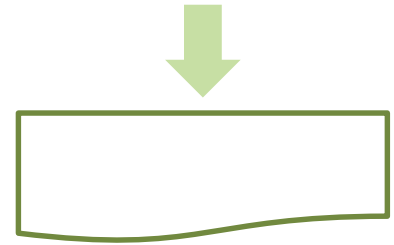
Риски ИБ и Риски информационных систем

- ✓ Реализация программ контроля (программ аудита)
- ✓ Тестирование на проникновение
- ✓ Мониторинг рисков ИБ
- ✓ Контроль КПУР
- ✓ Независимая оценка на ежегодной основе (например, службой внутреннего аудита)



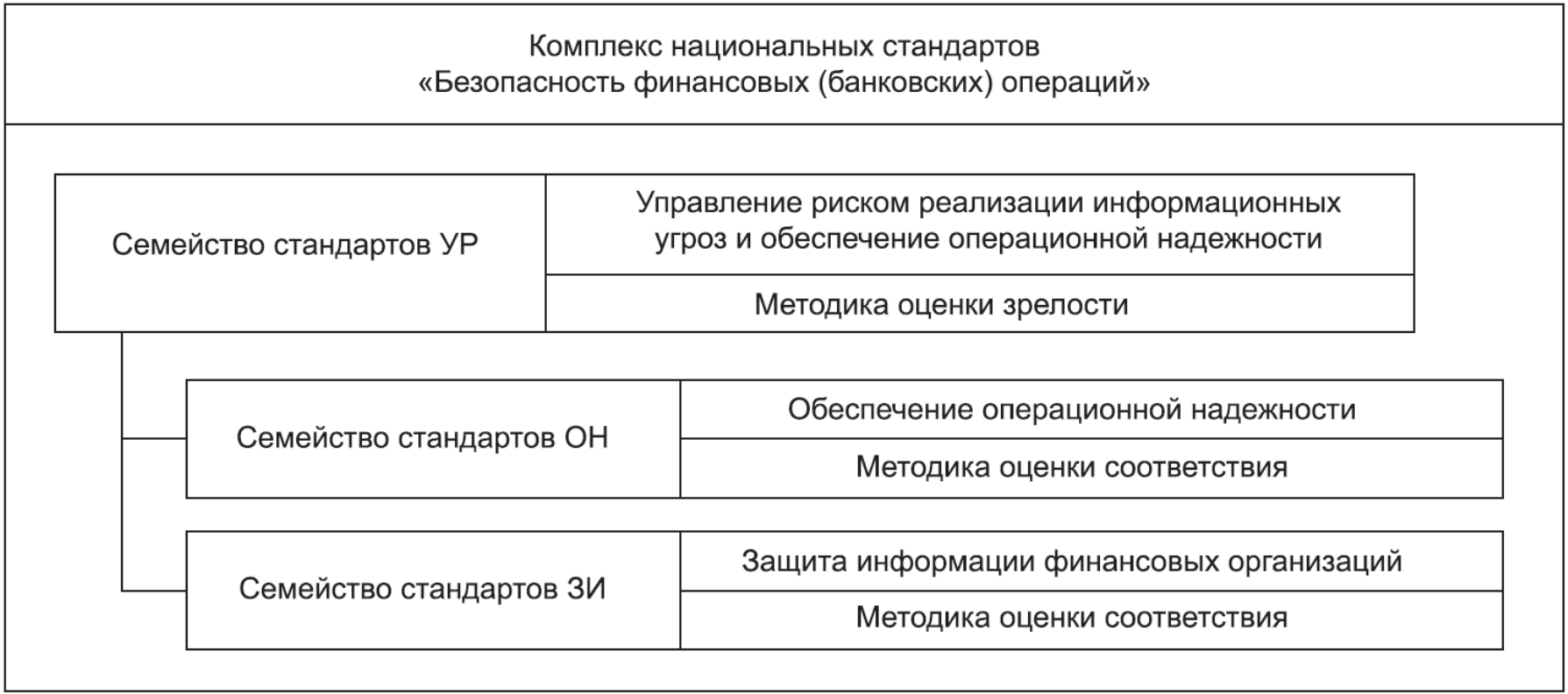
Отчетность на периодической основе

- ✓ Тестирование на проникновение
- ✓ Оценка достаточности и эффективности используемых информационных систем
- ✓ Проведение независимой оценки качества данных (не реже 1 раза в год)
- ✓ Независимая оценка на ежегодной основе (например, службой внутреннего аудита)

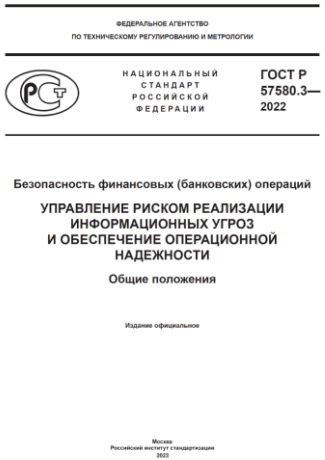


Отчетность на периодической основе

Комплекс стандартов ГОСТ Р 57580.х



ГОСТ Р 57580.3-2022


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 57580.3— 2022

Безопасность финансовых (банковских) операций

УПРАВЛЕНИЕ РИСКОМ РЕАЛИЗАЦИИ ИНФОРМАЦИОННЫХ УГРОЗ И ОБЕСПЕЧЕНИЕ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

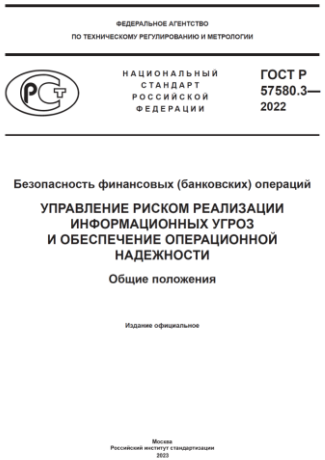
Общие положения

Издание официальное

Москва
Российский институт стандартизации
2022

Устанавливает требования к системе управления **риском реализации информационных угроз**

ГОСТ Р 57580.3-2022


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 57580.3— 2022

Безопасность финансовых (банковских) операций

УПРАВЛЕНИЕ РИСКОМ РЕАЛИЗАЦИИ ИНФОРМАЦИОННЫХ УГРОЗ И ОБЕСПЕЧЕНИЕ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

Общие положения

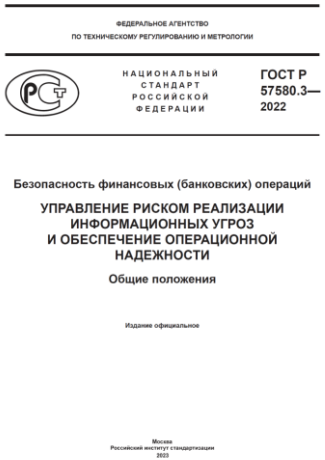
Издание официальное

Москва
Российский институт стандартизации
2023

Устанавливает требования к системе управления **риском реализации информационных угроз**

Направлено на обеспечение операционной надежности

ГОСТ Р 57580.3-2022


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 57580.3— 2022

Безопасность финансовых (банковских) операций

УПРАВЛЕНИЕ РИСКОМ РЕАЛИЗАЦИИ ИНФОРМАЦИОННЫХ УГРОЗ И ОБЕСПЕЧЕНИЕ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

Общие положения

Издание официальное

Москва
Российский институт стандартизации
2022

Устанавливает требования к системе управления **риском реализации информационных угроз**

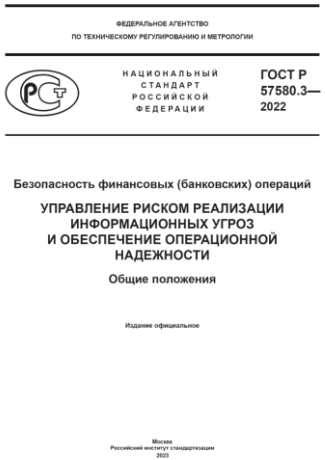
↓

Направлено на обеспечение операционной надежности

↓

Связано с бизнес-процессами (технологическими процессами) и объектами информатизации

ГОСТ Р 57580.3-2022


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 57580.3— 2022

Безопасность финансовых (банковских) операций

УПРАВЛЕНИЕ РИСКОМ РЕАЛИЗАЦИИ ИНФОРМАЦИОННЫХ УГРОЗ И ОБЕСПЕЧЕНИЕ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

Общие положения

Издание официальное

Москва
Российский институт стандартизации
2022

Устанавливает требования к системе управления **риском реализации информационных угроз**

↓

Направлено на обеспечение операционной надежности

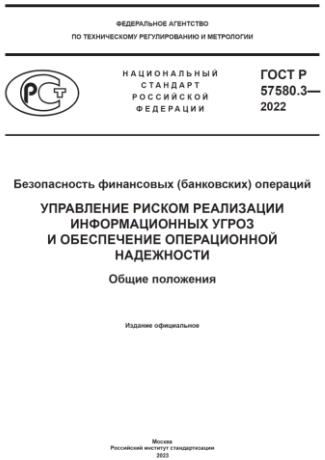
↓

Связано с бизнес-процессами (технологическими процессами) и объектами информатизации

↓

Реализуется в «классической» модели PDCA

ГОСТ Р 57580.3-2022


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 57580.3— 2022

Безопасность финансовых (банковских) операций

УПРАВЛЕНИЕ РИСКОМ РЕАЛИЗАЦИИ ИНФОРМАЦИОННЫХ УГРОЗ И ОБЕСПЕЧЕНИЕ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

Общие положения

Издание официальное

Москва
Российский институт стандартизации
2022

Устанавливает требования к системе управления **риском реализации информационных угроз**

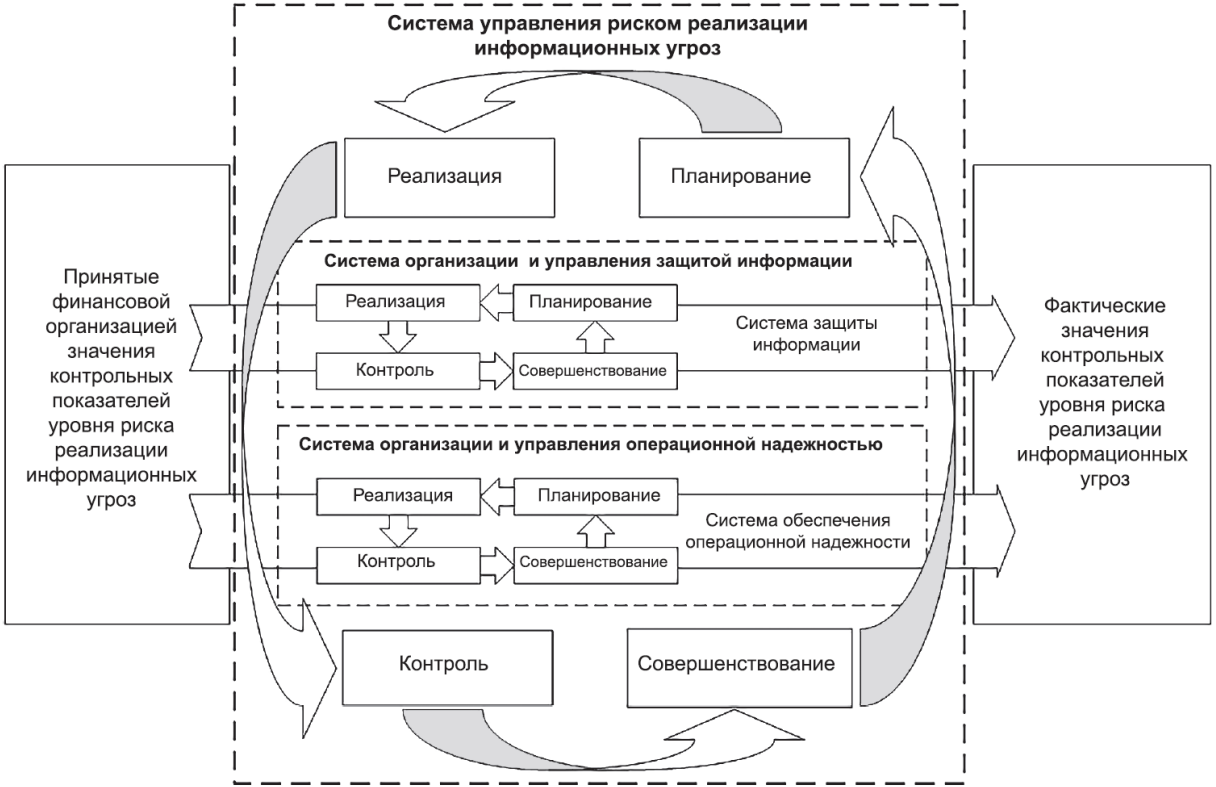
Направлено на обеспечение операционной надежности

Связано с бизнес-процессами (технологическими процессами) и объектами информатизации

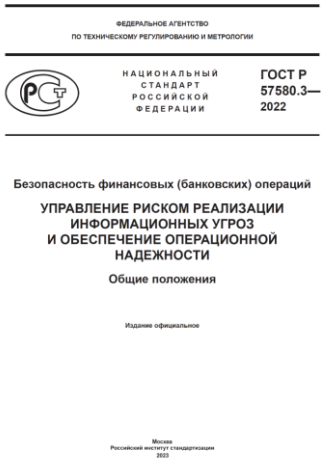
Реализуется в «классической» модели PDCA

Интегрировано в общую систему управления операционным риском

ГОСТ Р 57580.3-2022



ГОСТ Р 57580.3-2022



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 57580.3— 2022

Безопасность финансовых (банковских) операций

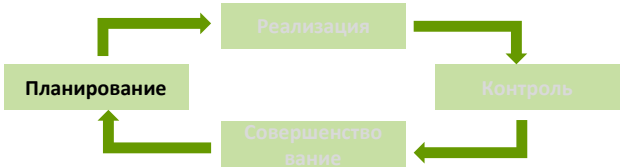
УПРАВЛЕНИЕ РИСКОМ РЕАЛИЗАЦИИ ИНФОРМАЦИОННЫХ УГРОЗ И ОБЕСПЕЧЕНИЕ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

Общие положения

Издание официальное

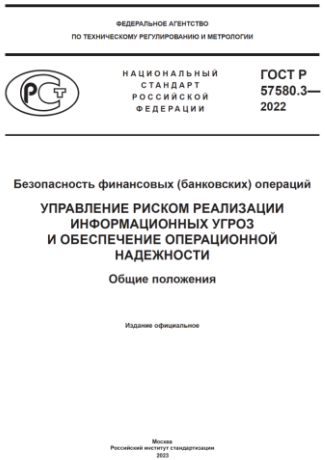
Москва
Российский институт стандартизации
2023

Требования к системе управления риском реализации информационных угроз



- ✓ определение политики управления риском реализации информационных угроз (с учетом требований ГОСТ Р 57580.3-2022 и Положения Банка России 716-П)
  - ✓ установление структуры и организации системы управления риском реализации информационных угроз, а также распределение функций, ролей и ответственности в рамках управления риском реализации информационных угроз;
  - ✓ установление политики управления риском реализации информационных угроз;
  - ✓ участие совета директоров (наблюдательного совета) и коллегиального исполнительного органа финансовой организации в решении вопросов управления риском реализации информационных угроз
- ✓ выявление и идентификацию риска реализации информационных угроз, а также его оценку;
  - ✓ идентификация критичной архитектуры;
  - ✓ идентификация риска реализации информационных угроз;
  - ✓ выявление и моделирование информационных угроз;
  - ✓ оценка риска реализации информационных угроз
- ✓ организация ресурсного (кадрового и финансового) обеспечения:
  - ✓ организация ресурсного (кадрового и финансового) обеспечения процессов системы управления риском реализации информационных угроз;
  - ✓ организация ресурсного (кадрового и финансового) обеспечения функционирования службы ИБ;
  - ✓ организация целевого обучения по вопросам выявления и противостояния реализации информационных угроз

ГОСТ Р 57580.3-2022


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 57580.3— 2022

Безопасность финансовых (банковских) операций

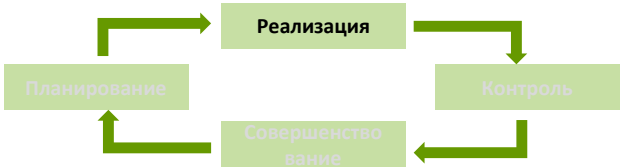
УПРАВЛЕНИЕ РИСКОМ РЕАЛИЗАЦИИ ИНФОРМАЦИОННЫХ УГРОЗ И ОБЕСПЕЧЕНИЕ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

Общие положения

Издание официальное

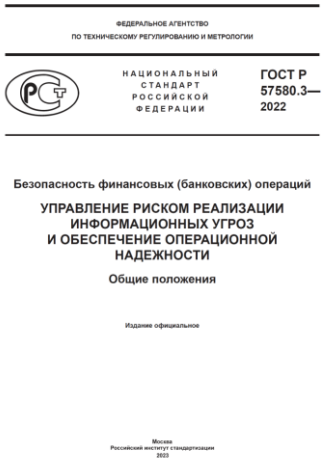
Москва
Российский институт стандартизации
2022

Требования к системе управления риском реализации информационных угроз



- ✓ разработка мероприятий, направленных на уменьшение негативного влияния риска реализации информационных угроз
  - ✓ выбор и применение способа реагирования на риск реализации информационных угроз;
  - ✓ разработка мероприятий, направленных на снижение СВР инцидентов;
  - ✓ разработка мероприятий, направленных на ограничение СТП инцидентов
- ✓ защита от информационных угроз (рекомендуется использовать меры из ГОСТ Р 57580.1-2017)
  - ✓ защита информации финансовой организации;
  - ✓ операционная надежность;
  - ✓ управление риском реализации информационных угроз при аутсорсинге и взаимодействии с поставщиками услуг;
  - ✓ управление риском внутреннего нарушителя;
  - ✓ управление риском реализации информационных угроз в финансовой экосистеме;
  - ✓ выполнение мероприятий, направленных на предотвращение утечек информации
- ✓ реагирование на инциденты, связанные с реализацией информационных угроз, и восстановление после их реализации;
- ✓ выявление событий риска реализации информационных угроз:
  - ✓ сбор и регистрацию информации о внутренних событиях риска реализации информационных угроз и потерях;
  - ✓ выявление и фиксацию инцидентов, в том числе обнаружение реализации компьютерных атак и выявление фактов (индикаторов) компрометации объектов информатизации;
  - ✓ ведение претензионной работы
- ✓ обеспечение осведомленности об актуальных информационных угрозах

ГОСТ Р 57580.3-2022



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 57580.3— 2022

Безопасность финансовых (банковских) операций

УПРАВЛЕНИЕ РИСКОМ РЕАЛИЗАЦИИ ИНФОРМАЦИОННЫХ УГРОЗ И ОБЕСПЕЧЕНИЕ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

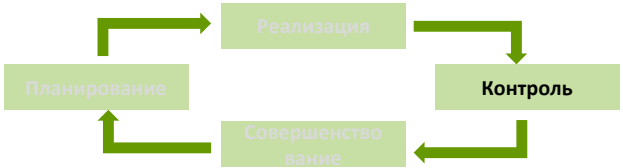
Общие положения

Издание официальное

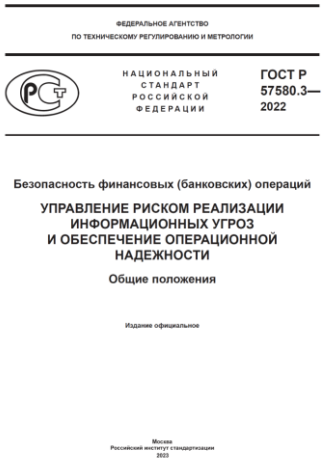
Москва
Российский институт стандартизации
2023

- ✓ установление и реализация программ контроля и аудита
  - ✓ проведение самооценки и профессиональной независимой оценки зрелости процессов обеспечения операционной надежности и защиты информации (самооценка для организаций по минимальному ровню);
  - ✓ проведение сценарного анализа (в части возможной реализации информационных угроз) и тестирования с использованием его результатов готовности финансовой организации противостоять реализации информационных угроз в отношении критичной архитектуры (киберучения)
  - ✓ оценка эффективности функционирования системы управления риском реализации информационных угроз
  - ✓ организацию внутренней отчетности в рамках управления риском реализации информационных угроз
- ✓ мониторинг риска реализации информационных угроз

Требования к системе управления риском реализации информационных угроз



ГОСТ Р 57580.3-2022



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 57580.3— 2022

Безопасность финансовых (банковских) операций

УПРАВЛЕНИЕ РИСКОМ РЕАЛИЗАЦИИ ИНФОРМАЦИОННЫХ УГРОЗ И ОБЕСПЕЧЕНИЕ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

Общие положения

Издание официальное

Москва
Российский институт стандартизации
2022

- ✓ обеспечение соответствия фактических значений КПУР принятым
  - ✓ проведение анализа необходимости совершенствования системы управления риском реализации информационных угроз;
  - ✓ принятие решений по совершенствованию системы управления риском реализации информационных угроз

Приложение. Классификация событий риска реализации информационных угроз и событий операционной надежности

Рассматриваемые технологические процессы:

- ✓ привлечение денежных средств физических лиц во вклады
- ✓ привлечение денежных средств юридических лиц во вклады
- ✓ размещение привлеченных во вклады денежных средств физических и (или) юридических лиц от своего имени и за свой счет
- ✓ осуществление переводов денежных средств по поручению физических лиц по их банковским счетам
- ✓ осуществление переводов денежных средств по поручению юридических лиц
- ✓ открытие и ведение банковских счетов физических лиц
- ✓ открытие и ведение банковских счетов юридических лиц
- ✓ осуществление переводов денежных средств без открытия банковских счетов
- ✓ выполнение операций на финансовых рынках
- ✓ выполнение кассовых операций
- ✓ работа онлайн-сервисов дистанционного обслуживания и доступа к осуществлению операций
- ✓ размещение и обновление биометрических персональных данных в единой биометрической системе
- ✓ идентификация и (или) аутентификация с использованием биометрических персональных данных физических лиц, в том числе с применением информационных технологий без их личного присутствия

Приложение. Классификация событий риска реализации информационных угроз и событий операционной надежности

Рассматриваемые технологические процессы:

- ✓ привлечение денежных средств физических лиц во вклады
- ✓ привлечение денежных средств юридических лиц во вклады
- ✓ размещение привлеченных во вклады денежных средств физических и (или) юридических лиц от своего имени и за свой счет
- ✓ осуществление переводов денежных средств по поручению физических лиц по их банковским счетам
- ✓ осуществление переводов денежных средств по поручению юридических лиц
- ✓ открытие и ведение банковских счетов физических лиц
- ✓ открытие и ведение банковских счетов юридических лиц
- ✓ осуществление переводов денежных средств без открытия банковских счетов
- ✓ выполнение операций на финансовых рынках
- ✓ выполнение кассовых операций
- ✓ работа онлайн-сервисов дистанционного обслуживания и доступа к осуществлению операций
- ✓ размещение и обновление биометрических персональных данных в единой биометрической системе
- ✓ идентификация и (или) аутентификация с использованием биометрических персональных данных физических лиц, в том числе с применением информационных технологий без их личного присутствия

Приложение. Классификация событий риска реализации информационных угроз и событий операционной надежности

Рассматриваемые технологические процессы:

- ✓ привлечение денежных средств физических лиц во вклады
- ✓ привлечение денежных средств юридических лиц во вклады
- ✓ размещение привлеченных во вклады денежных средств физических и (или) юридических лиц от своего имени и за свой счет
- ✓ осуществление переводов денежных средств по поручению физических лиц по их банковским счетам
- ✓ осуществление переводов денежных средств по поручению юридических лиц
- ✓ открытие и ведение банковских счетов физических лиц
- ✓ открытие и ведение банковских счетов юридических лиц
- ✓ осуществление переводов денежных средств без открытия банковских счетов
- ✓ выполнение операций на финансовых рынках
- ✓ выполнение кассовых операций
- ✓ работа онлайн-сервисов дистанционного обслуживания и доступа к осуществлению операций
- ✓ размещение и обновление биометрических персональных данных в единой биометрической системе
- ✓ идентификация и (или) аутентификация с использованием биометрических персональных данных физических лиц, в том числе с применением информационных технологий без их личного присутствия

Статья 5.1 (банковские операции) предусматривает еще следующие операции:

- ✓ купля-продажа иностранной валюты в наличной и безналичной формах
- ✓ привлечение драгоценных металлов физических и юридических лиц во вклады
- ✓ размещение привлеченных драгоценных металлов от своего имени и за свой счет
- ✓ открытие и ведение банковских счетов физических и юридических лиц в драгоценных металлах
- ✓ осуществление переводов по поручению физических и юридических лиц, в том числе банков-корреспондентов, по их банковским счетам в драгоценных металлах

ГОСТ Р 57580.3-2022

Приложения к ГОСТ Р 57580.3-2022 детализируют состав КПУР для кредитных и некредитных финансовых организаций:

- ✓ КПУР, характеризующие уровень совокупных потерь кредитной организации в результате инцидентов (связанные с суммами потерь)
- ✓ КПУР, характеризующие уровень несанкционированных операций в результате инцидентов (связанные либо с суммами операций, либо с их количествами)
- ✓ КПУР, характеризующие уровень зрелости процессов обеспечения операционной надежности и защиты информации

ГОСТ Р 57580.3-2022

Приложения к ГОСТ Р 57580.3-2022 детализируют состав КПУР для кредитных и некредитных финансовых организаций:

- ✓ КПУР, характеризующие уровень совокупных потерь кредитной организации в результате инцидентов (связанные с суммами потерь)
- ✓ КПУР, характеризующие уровень несанкционированных операций в результате инцидентов (связанные либо с суммами операций, либо с их количествами)
- ✓ КПУР, характеризующие уровень зрелости процессов обеспечения операционной надежности и защиты информации

Уровень зрелости процессов планирования, реализации, контроля и совершенствования системы защиты информации, определяемой в соответствии с ГОСТ Р 57580.1 (ТН) и ГОСТ Р 57580.4

Уровень зрелости процесса «Обеспечение защиты информации при управлении доступом»

Уровень зрелости процесса «Предотвращение утечек информации»

Уровень зрелости процессов применения технологических мер защиты информации (12-МР?)

Уровень зрелости процессов реализации функций безопасности и уязвимостей объектов информатизации прикладного уровня (12-МР?)

Оценка эффективности функционирования системы управления риском реализации информационных угроз (оценка соответствия требованиям ГОСТ Р 57580.3? или 716-П?)

Спасибо за внимание!
Вопросы?

АО «ДиалогНаука»
Телефон: +7 (495) 980-67-76
Факс: +7 (495) 980-67-75
E-mail: svintsitskii@dialognauka.ru

http://www.DialogNauka.ru