ОБЗОР И ПРАКТИКА ПРИМЕНЕНИЯ НАЦИОНАЛЬНОГО СТАНДАРТА ГОСТ Р 57580.1-2017

Антон Свинцицкий
Директор по консалтингу
АО «ДиалогНаука»

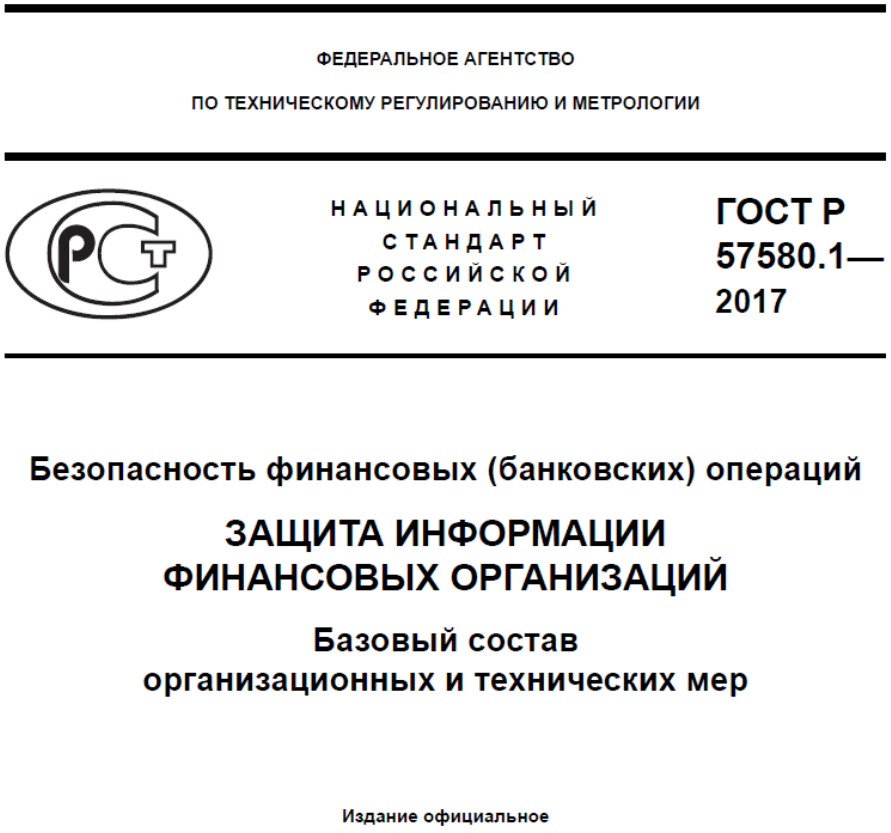
Москва, 13 октября 2020 года

ДиалогНаука

Содержание

1. Обзор стандарта
2. Как правильно определить контуры безопасности и выбрать уровень защиты
3. Базовые требования по защите информации
4. Необходимость выполнения требований для кредитных и некредитных финансовых организаций (Положения Банка России 672-П, 683-П и 684-П)

Обзор национального стандарта ГОСТ Р 57580.1-2017



ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 57580.1— 2017

Безопасность финансовых (банковских) операций

ЗАЩИТА ИНФОРМАЦИИ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

Базовый состав организационных и технических мер

Издание официальное

УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 822-ст

ГОСТ Р 57580.1-2017

ГОСТ Р 57580.1-2017

ГОСТ Р 57580.1-2017

Определение контуров безопасности

Цитата:

«Базовый состав мер защиты информации, определяемый настоящим стандартом, применим к совокупности объектов информатизации, в том числе автоматизированным системам (АС), используемым финансовыми организациями для выполнения бизнес-процессов и (или) технологических процессов, связанных с предоставлением финансовых, банковских услуг, а также услуг по осуществлению переводов денежных средств».

Определение контуров безопасности

Цитата:

«Базовый состав мер защиты информации, определяемый настоящим стандартом, применим к совокупности объектов информатизации, в том числе автоматизированным системам (АС), используемым финансовыми организациями для выполнения бизнес-процессов и (или) технологических процессов, связанных с предоставлением финансовых, банковских услуг, а также услуг по осуществлению переводов денежных средств».

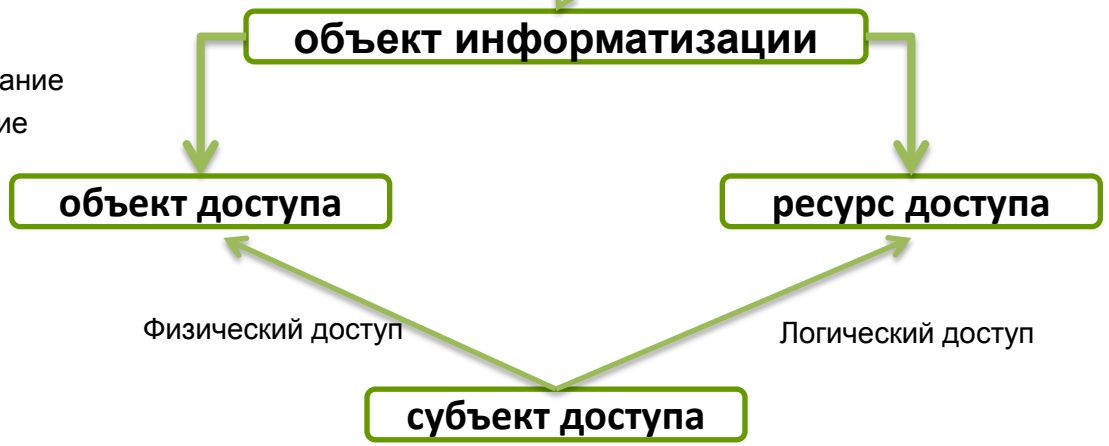
Статья 5 Федерального закона «О банках и банковской деятельности»:

- ✓ Привлечение денежных средств физических и юридических лиц во вклады (до востребования и на определенный срок)
- ✓ Открытие и ведение банковских счетов физических и юридических лиц
- ✓ Осуществление переводов денежных средств по поручению физических и юридических лиц, в том числе банков-корреспондентов, по их банковским счетам
- ✓ Инкассация денежных средств, векселей, платежных и расчетных документов и кассовое обслуживание физических и юридических лиц
- ✓ (Примечание: инкассация исключена из области оценки в соответствии с дополнительными разъяснениями Банка России)
- ✓ Купля - продажа иностранной валюты в наличной и безналичной формах
- ✓ Привлечение драгоценных металлов физических и юридических лиц во вклады (до востребования и на определенный срок), за исключением монет из драгоценных металлов
- ✓ Открытие и ведение банковских счетов физических и юридических лиц в драгоценных металлах, за исключением монет из драгоценных металлов
- ✓ Осуществление переводов по поручению физических и юридических лиц, в том числе банков-корреспондентов, по их банковским счетам в драгоценных металлах
- ✓ Осуществление переводов денежных средств без открытия банковских счетов, в том числе электронных денежных средств (за исключением почтовых переводов)
- ✓ …

Определение контуров безопасности

Цитата:

«Базовый состав мер защиты информации, определяемый настоящим стандартом, применим к совокупности объектов информатизации, в том числе автоматизированным системам (АС), используемым финансовыми организациями для выполнения бизнес-процессов и (или) технологических процессов, связанных с предоставлением финансовых, банковских услуг, а также услуг по осуществлению переводов денежных средств».



- ✓ АРМ пользователей
- ✓ Серверное оборудование
- ✓ Сетевое оборудование
- ✓ СХД
- ✓ HSM
- ✓ Принтеры и копиры
- ✓ ТУ ДБО

- ✓ АС
- ✓ БД
- ✓ Сетевые ресурсы
- ✓ Виртуальные машины
- ✓ Сервисы (электронная почта, WEB)

- ✓ Пользователь
- ✓ Клиент
- ✓ Эксплуатационный персонал
- ✓ Технический персонал
- ✓ Программный сервис

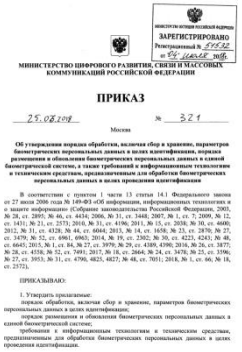
Определение контуров безопасности

Цитата:

«Базовый состав мер защиты информации, определяемый настоящим стандартом, применим к совокупности объектов информатизации, в том числе автоматизированным системам (АС), используемым финансовыми организациями для выполнения бизнес-процессов и (или) технологических процессов, связанных с предоставлением финансовых, банковских услуг, а также услуг по осуществлению переводов денежных средств».

Совокупность объектов информатизации

Необходимо обеспечить идентификацию и учет идентификацию и учет объектов информатизации, в том числе АС, включаемых в область применения стандарта



МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

25.06.2018 № 321

Москва

Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных в целях идентификации, порядка размещения и обновления биометрических персональных данных в единой биометрической системе, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации

В соответствии с пунктом 1 части 13 статьи 14.1 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (Собрание законодательства Российской Федерации, 2003, № 28, ст. 2895; № 46, ст. 4434; 2006, № 31, ст. 3448; 2007, № 1, ст. 7; 2009, № 12, ст. 1431; № 21, ст. 2573; 2010, № 31, ст. 4196; 2011, № 15, ст. 2038; № 30, ст. 4600; 2012, № 31, ст. 4328; № 44, ст. 6044; 2013, № 14, ст. 1658; № 23, ст. 2870; № 27, ст. 3479; № 52, ст. 6961, 6963; 2014, № 19, ст. 2302; № 30, ст. 4223, 4243; № 48, ст. 6643; 2015, № 1, ст. 84, № 27, ст. 3979; № 29, ст. 4389, 4390; 2016, № 26, ст. 3877; № 28, ст. 4558; № 52, ст. 7491; 2017, № 18, ст. 2664; № 24, ст. 3478; № 25, ст. 3596; № 27, ст. 3953; № 31, ст. 4790, 4825, 4827; № 48, ст. 7051; 2018, № 1, ст. 66; № 18, ст. 2572),

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемые:

порядок обработки, включая сбор и хранение, параметров биометрических персональных данных в целях идентификации;

порядок размещения и обновления биометрических персональных данных в единой биометрической системе;

требования к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации.

Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 25.06.2018 г. № 321

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ (БАНК РОССИИ)

ПОЛОЖЕНИЕ

О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств

Положения Банка России:

- ✓ 672-П
- ✓ 683-П
- ✓ 684-П
- ✓ 719-П

Методические рекомендации

- ✓ 4-МР

Определение контуров безопасности

Цитата:

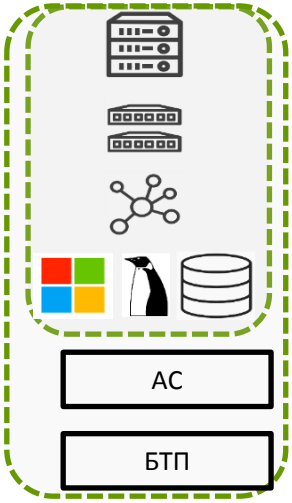
«Базовый состав мер защиты информации, определяемый настоящим стандартом, применим к совокупности объектов информатизации, в том числе автоматизированным системам (АС), используемым финансовыми организациями для выполнения бизнес-процессов и (или) технологических процессов, связанных с предоставлением финансовых, банковских услуг, а также услуг по осуществлению переводов денежных средств».

Совокупность объектов информатизации

Уровни информационной инфраструктуры:

- ✓ Системный уровень
- ✓ Уровень АС и приложений

- Уровень взаимодействия с клиентами кредитной организации (ФЛ и ЮЛ)
- Обработка ЭС в кредитной организации
- Работы с карточными данными
- Управление банкоматной сетью и платежными терминалами
- Системы взаимодействия с платежными системами (ССНП, СБП и иные ПС)
- Автоматизация функций оператора услуг платежной инфраструктуры (РЦ, ОЦ, КЦ)
- и другие...



- Инфраструктура
- Системы защиты информации

Определение контуров безопасности

Цитата:

«Базовый состав мер защиты информации, определяемый настоящим стандартом, применим к совокупности объектов информатизации, в том числе автоматизированным системам (АС), используемым финансовыми организациями для выполнения бизнес-процессов и (или) технологических процессов, связанных с предоставлением финансовых, банковских услуг, а также услуг по осуществлению переводов денежных средств».

Единая степень критичности
Единая политика защиты информации

Контур безопасности

Определение уровней защиты информации

Определение уровня защиты

- Минимальный (3)
- Стандартный (2)
- Усиленный (1)

Устанавливается нормативными актами Банк России

№ п/п	Контур безопасности	Нормативный документ	Уровень защиты информации	Критерий
1	ЕБС. Технологический участок сбора биометрических ПДн	п.5 Приложения 3 Приказа Министерства цифрового развития, связи и массовых коммуникаций РФ от 25 июня 2018 г. N 321 п.2.1.2 Методические рекомендации Банка России от 14 февраля 2019 г. № 4-МР	2	Все кредитные организации
2	ЕБС. Технологический участок обработки собранных биометрических персональных данных физических лиц с целью передачи в ЕБС	п.5 Приложения 3 Приказа Министерства цифрового развития, связи и массовых коммуникаций РФ от 25 июня 2018 г. N 321	2	Все кредитные организации
3		п.2.3.2 Методические рекомендации Банка России от 14 февраля 2019 г. № 4-МР	2	Все кредитные организации
4		п.2.3.3 Методические рекомендации Банка России от 14 февраля 2019 г. № 4-МР	1	Системно значимые кредитные организации
5	Участок осуществления переводов денежных средств с использованием ССНП	п.3 Положения Банка России 672-П	2	Все кредитные организации
6	Участок осуществления переводов денежных средств с использованием СБП	п.4 Положения Банка России 672-П	2	Все кредитные организации
7	Автоматизированные системы и объекты среды обработки защищаемой информации (информации о переводах денежных средств)	п.3.1 Положения Банка России 683-П	2	Все кредитные организации
8			1	Системно значимые кредитные организации, кредитные организации, выполняющие функции оператора услуг платежной инфраструктуры системно значимых платежных систем, кредитные организации, значимые на рынке платежных услуг,

Определение уровней защиты информации

Определение уровня защиты

- Минимальный (3)
- Стандартный (2)
- Усиленный (1)

Устанавливается нормативными актами Банк России

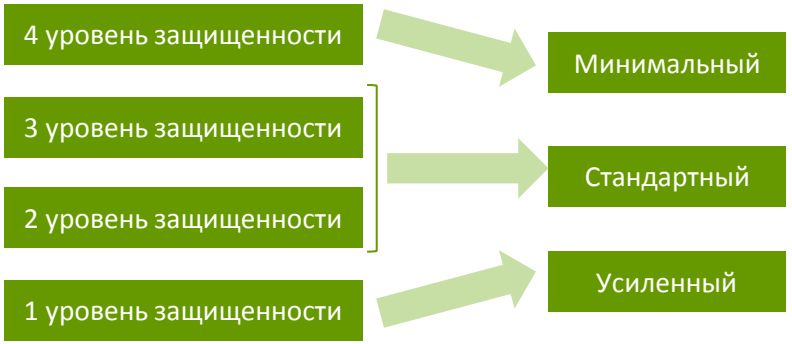
№ п/п	Контур безопасности
1	Автоматизированные системы и объекты среды обработки защищаемой информации (защищаемая информация в соответствии с п.1 Положения Банка России 684-П)
2	
3	

Положение Банка России от 4 июня 2020 г. N 719-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»

№ п/п 719-П	Требования (выдержка)	Категории субъектов					
		ОПДС	БПА	ОУИО	ППП	ОПС	ОУПИ
1.1	Реализация для объектов информационной инфраструктуры требований ГОСТ Р 57580.1-2017	+	+	+			+
Уровень защиты информации в соответствии с ГОСТ Р 57580.1-2017							
3.5	минимальный		+				
2.1 4.3 6.5	стандартный	+		+			+ Для остальных ПС
2.1 6.5	усиленный	+ для системно значимых КО					+ Для системно значимых ПС
2.4 3.7 4.5 6.8	Обеспечение не ниже 4 уровня соответствия	+	+ Для платежных агрегаторов	+			+

Определение уровней защиты информации

Уровни защиты для ИСПДн (рекомендуется использовать)



В соответствии с Постановлением Правительства РФ ПП-1119

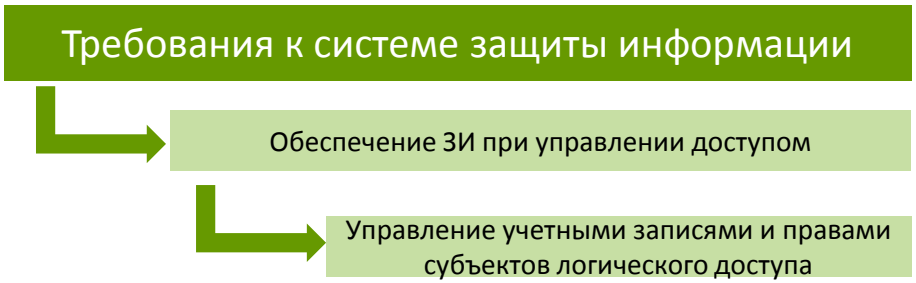
Базовые требования

Требования к системе защиты информации

Обеспечение ЗИ при управлении доступом

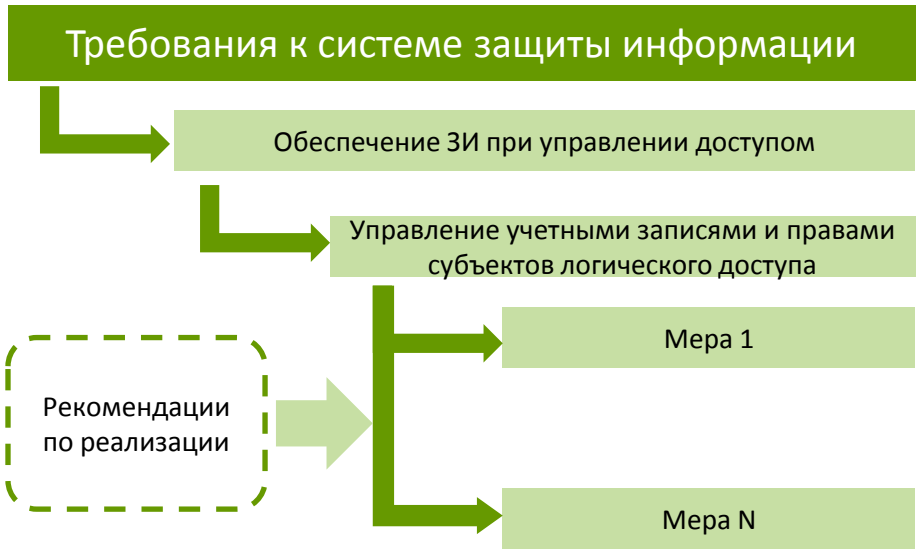
Направление	3 направления
Процесс	8 процессов

Базовые требования



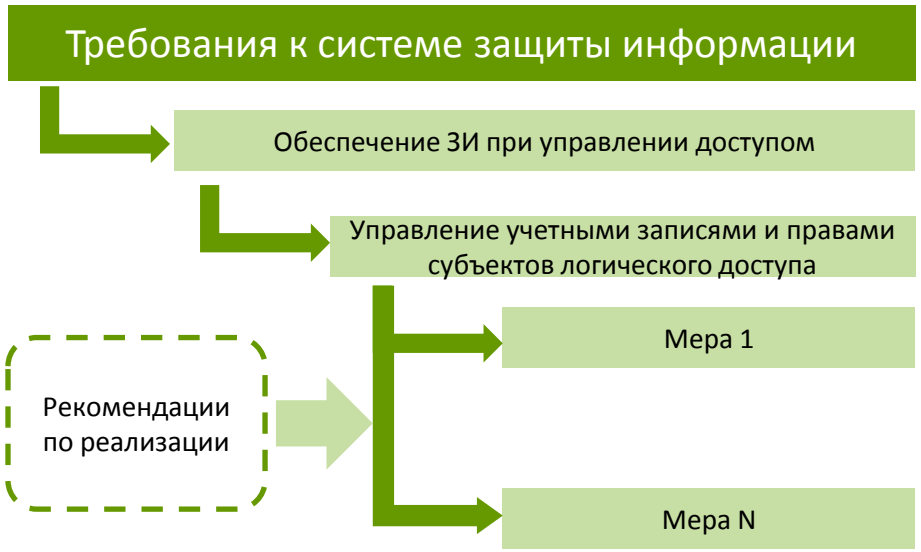
Направление	3 направления
Процесс	8 процессов
Подпроцесс	

Базовые требования



Направление	3 направления
Процесс	8 процессов
Подпроцесс	
Меры системы защиты информации	343 меры

Базовые требования



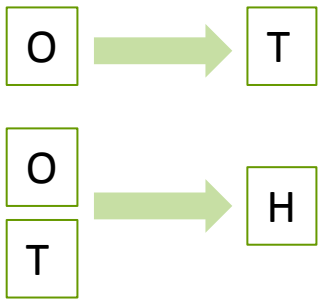
Направление — 3 направления

Процесс — 8 процессов

Подпроцесс

Меры системы защиты информации — 343 меры

Примечание:



Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
УЗП.5	Документарное определение правил предоставления (отзыва) и блокирования логического доступа	Н	О	О
УЗП.6	Назначение для всех ресурсов доступа распорядителя логического доступа (владельца ресурса доступа)	О	О	О
УЗП.7	Предоставление прав логического доступа по решению распорядителя логического доступа (владельца ресурса доступа)	О	О	О
УЗП.8	Хранение эталонной информации о предоставленных правах логического доступа и обеспечение целостности указанной информации	О	Т	Т

Базовые требования

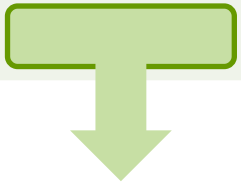
Положение Банка России 382-П

СТО БР ИББС 1.0-2014

Базовые требования

Базовые требования по каждому процессу лучше разбить по уровням среды обработки и оценивать их применимость и целесообразность для каждого уровня

Условное обозначение и номер меры	Применение меры на уровнях среды обработки				
	Аппаратное обеспечение	Сетевое оборудование	ОС	СУБД	…



Если мера не может быть реализована, то необходимо рассмотреть возможность/необходимость применения компенсирующих мер, направленных на обработку рисков, связанных с реализацией тех же угроз безопасности (с учетом Приложение А. Основные положения базовой модели угроз и нарушителей безопасности информации);

! Выбор компенсирующих мер должен быть формализован.
Стоит обратить внимание, что часть мер дополняет друг друга и могут быть использованы как компенсирующие…

Раздел 8 ГОСТ Р 57580.1-2017

Организационные меры защиты информации

ПЗИ.1 Область применения процесса

ПЗИ.2 Состав и содержание

ПЗИ.4 Порядок применения

Технические меры защиты информации

ПЗИ.3 Состав и содержание

ПЗИ.5 Порядок применения

Раздел 8 ГОСТ Р 57580.1-2017

Реализация организационных мер защиты информации

РЗИ.7 Применения мер

РЗИ.16 Повышение осведомленности

РЗИ.1 Учет объектов доступа и ресурсов доступа

РЗИ.4 Назначение на роли

РЗИ.15 Обучение

Реализация технических мер защиты информации

РЗИ.11-14 Сертифицированные СЗИ

РЗИ.8 Централизованное управление

РЗИ.9 Обеспечение доступности

РЗИ.2 Размещение и настройка

РЗИ.3 Контроль (тестирование)

Раздел 8 ГОСТ Р 57580.1-2017

Организационные меры защиты информации

КЗИ.1 Контроль состава объектов доступа и ресурсов доступа

КЗИ.5 Контроль

КЗИ.7 Проверка знаний

Технические меры защиты информации

КЗИ.2-3 Контроль эксплуатации

КЗИ.4 Периодический контроль

Раздел 8 ГОСТ Р 57580.1-2017

- ✓ обнаружения инцидентов защиты информации;
- ✓ обнаружения недостатков в рамках контроля системы защиты информации;
- ✓ изменения политики финансовой организации;
- ✓ изменений требований к защите информации, определенных правилами платежной системы;
- ✓ изменений, внесенных в законодательство Российской Федерации, в том числе нормативные акты Банка России

Спасибо за внимание!
Вопросы?

Свинцицкий Антон Игоревич

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

http://www.DialogNauka.ru

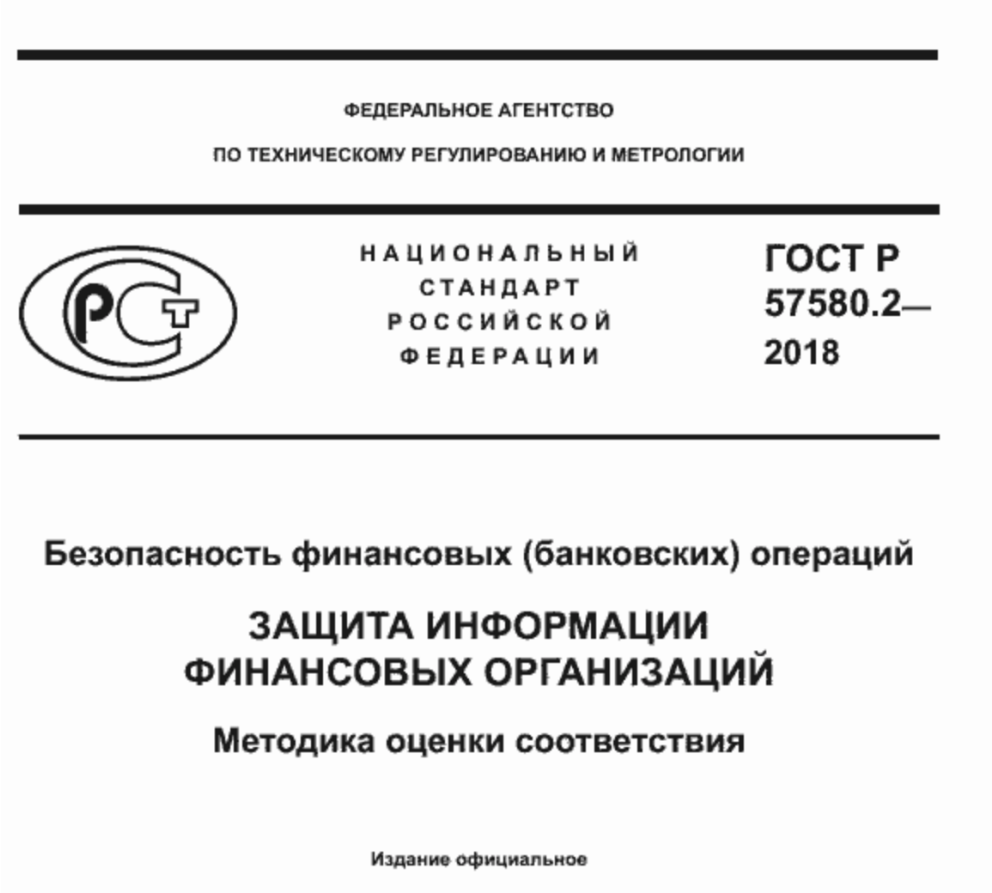
ОСОБЕННОСТИ ПРОВЕДЕНИЯ ОЦЕНКИ СООТВЕТСТВИЯ ПО ГОСТ Р 57580.1-2018

Антон Свинцицкий
Директор по консалтингу
АО «ДиалогНаука»

Москва, 13 октября 2020 года

ДиалогНаука

ГОСТ Р 57580.1-2017



ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 57580.2— 2018

Безопасность финансовых (банковских) операций

ЗАЩИТА ИНФОРМАЦИИ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

Методика оценки соответствия

Издание официальное

УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 28 марта 2018 г. № 156-ст

Методика оценки соответствия

- ✓ Оценка выбора и реализации финансовой организацией организационных и технических мер ЗИ в соответствии с требованиями ГОСТ Р 57580.1-2017 проводится независимой организацией:
  - обладающей необходимой компетенцией (как оценить?)
  - обладающей лицензией на деятельность по технической защите конфиденциальной информации

- ✓ Оценка осуществляется по следующим основным направлениям:
  - выбор финансовой организацией организационных и технических мер ЗИ, направленных на непосредственное обеспечение ЗИ (раздел 7 ГОСТ)
  - полнота реализации организационных и технических мер ЗИ, направленных на непосредственное обеспечение ЗИ и входящих в систему организации и управления ЗИ (раздел 8 ГОСТ)
  - обеспечение ЗИ на этапах жизненного цикла АС (раздел 9 ГОСТ)

Схема оценки

Шаг 1.

1. Определение области оценки (должна совпадать с областью применения ГОСТ Р 57580.1)

- Типы защищаемой информации в соответствии с требованиями нормативных документов
- Банковские технологические процессы
- Объекты информационной инфраструктуры

- Уровень взаимодействия с клиентами кредитной организации (ФЛ и ЮЛ)
- Обработка ЭС в кредитной организации
- Работы с карточными данными
- Управление банкоматной сетью и платежными терминалами
- Системы взаимодействия с платежными системами (ССНП, СБП и иные ПС)
- Автоматизация функций оператора услуг платежной инфраструктуры (РЦ, ОЦ, КЦ)
- и другие...

- Инфраструктура
- Системы защиты информации

Область применения требований  Репрезентативная выборка

Схема оценки

Шаг 1.

1. Определение области оценки (должна совпадать с областью применения ГОСТ Р 57580.1)

Шаг 2.

1. Формирование перечня неоцениваемых показателей:
   - ✓ связанные с неиспользуемыми информационными технологиями (например, беспроводные сети)
   - ✓ реализация которых не является необходимой для нейтрализации актуальных угроз безопасности, определенных в модели угроз и нарушителей
   - ✓ добавление в реестр оценки компенсирующих мер

Схема оценки

Шаг 1.

1. Определение области оценки (должна совпадать с областью применения ГОСТ Р 57580.1)

Шаг 2.

1. Формирование перечня неоцениваемых показателей:
   - ✓ связанные с неиспользуемыми информационными технологиями (например, беспроводные сети)
   - ✓ реализация которых не является необходимой для нейтрализации актуальных угроз безопасности, определенных в модели угроз и нарушителей
   - ✓ добавление в реестр оценки компенсирующих мер

методика проверки модели угроз?

Схема оценки

Шаг 1.

1. Определение области оценки (должна совпадать с областью применения ГОСТ Р 57580.1)

Шаг 2.

1. Формирование перечня неоцениваемых показателей:
   - ✓ связанные с неиспользуемыми информационными технологиями (например, беспроводные сети)
   - ✓ реализация которых не является необходимой для нейтрализации актуальных угроз безопасности, определенных в модели угроз и нарушителей
   - ✓ добавление в реестр оценки компенсирующих мер

методика проверки модели угроз?

как оценить полноту компенсирующих мер?

Схема оценки

Шаг 3.

1. Сбор информации и свидетельств выполнения (реализации) мер:

- ✓ документы проверяемой организации и иные материалы проверяемой организации в бумажном или электронном виде (при необходимости, документы третьих лиц)
- ✓ устные высказывания сотрудников проверяемой организации в процессе проводимых опросов в области оценки соответствия ЗИ;
- ✓ результаты наблюдений членов проверяющей группы за процессами системы ЗИ и деятельностью сотрудников проверяемой организации в области оценки соответствия ЗИ;
- ✓ параметры конфигураций и настроек технических объектов информатизации и средств ЗИ;
- ✓ технические методы, технические и программные средства сбора свидетельств полноты реализации мер ЗИ (анализ электронных журналов регистрации, анализ фактических настроек, **анализ уязвимостей, проведение тестирования на проникновение** и т.п.)

Методика

Требования раздела 7
(Требования к системе защиты информации)

$$E_{МЗИ} = \begin{cases} 0, \text{мера не выбрана} \\ 1, \text{мера выбрана} \end{cases}$$

Требования раздела 8
(Требования к организации и управлению защитой информации)

$$E_{МОУ} = \begin{cases} 0 \\ 0{,}5 \\ 1 \end{cases}$$

Требования раздела 9
(Требования к защите информации на этапах ЖЦ)

$$E_{МАС} = \begin{cases} 0 \\ 0{,}5 \\ 1 \end{cases}$$

Методика

- **Процесс 1** Обеспечение защиты информации при управлении доступом
- **Процесс 2** Обеспечение защиты вычислительных сетей
- **Процесс 3** Контроль целостности и защищенности
- **Процесс 4** Защита от вредоносного кода
- **Процесс 5** Предотвращение утечек информации
- **Процесс 6** Управление инцидентами ЗИ
- **Процесс 7** Защита среды виртуализации
- **Процесс 8** Удаленный доступ и мобильные устройства

Подпроцесс 1

Подпроцесс N

$$\text{Е}_{\text{ППЗИ}_i} = \frac{\sum_{j=1}^{N} E_{\text{МЗИ}_j}}{N}$$

$$\text{Е}_{\text{ПЗИ}_i} = \frac{\sum_{k=1}^{T} E_{\text{ППЗИ}_K}}{T}$$

Применимо для процессов 1,2 и 6

$$\text{Е}_{\text{ПЗИ}_i} = \frac{\sum_{j=1}^{N} E_{\text{МЗИ}_j}}{N}$$

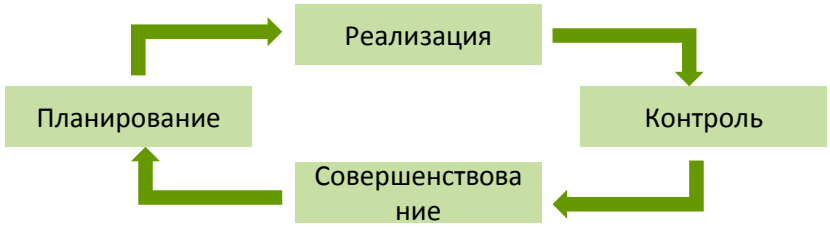
Например:

Для подпроцесса «Управление учетными записями и правами субъектов логического доступа»:

- ✓ Для уровня ЗИ = 3 $\text{Е}_{\text{ППЗИ}} = \frac{\sum_{j=1}^{22} E_{\text{МЗИ}_j}}{22}$
- ✓ Для уровня ЗИ = 2 $\text{Е}_{\text{ППЗИ}} = \frac{\sum_{j=1}^{27} E_{\text{МЗИ}_j}}{27}$

Методика

Требования к организации и управлению защитой информации



Данные требования применяются ко всем 8 процесса, а не к финансовой организации в целом

$$\mathrm{E}_{\Pi_i}\left(\mathrm{E}_{\mathrm{P}_i}, \mathrm{E}_{\mathrm{K}_i}, \mathrm{E}_{\mathrm{C}_i}\right) = \frac{\sum_{j=1}^{O} E_{\mathrm{МОУ}_j}}{O}$$

Требования к защите информации на этапах ЖЦ

$$E_{\mathrm{AC}} = \frac{\sum_{j=1}^{L} E_{\mathrm{MAC}_j}}{L}$$

Рекомендации по защите ПДн

Не оцениваются…

Методика

Требования к системе защиты информации

$$\mathrm{E}_{\mathrm{ПЗИ}_i} = \frac{\sum_{j=1}^{N} E_{\mathrm{МЗИ}_j}}{N}$$

$$E_i = \frac{\mathrm{E}_{\mathrm{ПЗИ}_i} + (0{,}2 * \mathrm{E}_{\mathrm{П}_i} + 0{,}4 * \mathrm{E}_{\mathrm{Р}_i} + 0{,}25 * \mathrm{E}_{\mathrm{К}_i} + 0{,}15 * \mathrm{E}_{\mathrm{С}_i})}{2}$$

Если в область оценки соответствия входят несколько контуров безопасности разного уровня

$$E_i = k_1 E_{1i} + k_2 E_{2i} + k_3 E_{3i}$$

Наличие контура заданного уровня			Корректирующий коэффициент		
3	2	1	E_{3i}	E_{2i}	E_{1i}
+	+	+	0,1	0,3	0,6
	+	+		0,3	0,7
+		+	0,2		0,8
+	+		0,4	0,6	

Интерпретация результатов оценки

Уровни соответствия	Результаты оценки E_i
Нулевой уровень соответствия	0
Первый уровень соответствия	$0 < E_i \leq 0{,}5$
Второй уровень соответствия	$0{,}5 < E_i \leq 0{,}7$
Третий уровень соответствия	$0{,}7 < E_i \leq 0{,}85$
Четвертый уровень соответствия	$0{,}85 < E_i \leq 0{,}9$
Пятый уровень соответствия	$0{,}9 < E_i$

Рекомендуемый ЦБ

Итоговая оценка соответствия ЗИ ***R***

$$R = \frac{\sum_{i=1}^{T} E_i + E_{\text{AC}}}{T+1} - 0{,}01 * Z$$

Требования к отчетным документам

Отчет о результатах оценки соответствия требованиям ГОСТ

- ✓ сведения о проверяющей организации
- ✓ сведения о руководителе и членах проверяющей группы
- ✓ сведения о проверяемой организации
- ✓ сведения о заказчике оценки соответствия ЗИ
- ✓ цель оценки соответствия ЗИ
- ✓ сроки проведения оценки соответствия ЗИ
- ✓ область оценки соответствия ЗИ
- ✓ перечень неоцениваемых областей оценки соответствия ЗИ (процессов системы ЗИ, подпроцессов системы ЗИ, направлений ЗИ, мер ЗИ) с обоснованием их исключения из области оценки соответствия ЗИ
- ✓ обоснование применения компенсирующих мер ЗИ при невозможности реализации отдельных выбранных мер ЗИ
- ✓ краткое изложение процесса оценки соответствия ЗИ, включая элемент неопределенности и (или) проблемы, которые могут отразиться на надежности заключения по результатам оценки соответствия ЗИ
- ✓ числовое значение итоговой оценки соответствия ЗИ, характеризующей соответствие ЗИ проверяемой организации установленным требованиям на дату завершения оценки соответствия ЗИ
- ✓ подтверждение, что цель оценки соответствия ЗИ достигнута в области оценки соответствия ЗИ
- ✓ неразрешенные разногласия между проверяющей группой и проверяемой организацией
- ✓ перечень и сведения о представителях проверяемой организации, которые сопровождали проверяющую группу при проведении оценки соответствия ЗИ
- ✓ сведения о конфиденциальном характере содержания отчета по результатам оценки соответствия ЗИ
- ✓ **опись документов (копий документов) на бумажных носителях**, прилагаемых к отчету по результатам оценки соответствия ЗИ, с указанием общего количества томов приложений, количества и наименований документов, а также количества листов в каждом из них
- ✓ **опись машинных носителей информации, прилагаемых к отчету** по результатам оценки соответствия ЗИ, с указанием их реквизитов (наименование, тип, учетный номер и т.п.) и содержащихся на них файлов данных, а также результатов вычисления по каждому из них хэш-функции, реализованной в соответствии с ГОСТ Р 34.11-2012

Требования к отчетным документам

В заключении:

Отчет по результатам оценки соответствия ЗИ должен иметь сквозную нумерацию страниц, регистрационный номер, должен быть прошит нитью, не имеющей разрывов, и скреплен печатью проверяющей организации с указанием количества листов в заверительной надписи, подписанной руководителем проверяющей .

Для каждого электронного документа, файла данных, прилагаемых к отчету по результатам оценки соответствия ЗИ, должны быть вычислены хэш-функции, реализованные в соответствии с ГОСТ Р 34.11

Периодичность оценки соответствия

№ п/п	Контур безопасности	Нормативный документ	Уровень защиты информации	Критерий	Срок вступления в силу	Периодичность
1	ЕБС. Технологический участок сбора биометрических ПДн	п.5 Приложения 3 Приказа Министерства цифрового развития, связи и массовых коммуникаций РФ от 25 июня 2018 г. N 321 п.2.1.2 Методические рекомендации Банка России от 14 февраля 2019 г. № 4-МР	2	Все кредитные организации	Вступило в силу	Ежегодно в соответствии с 321 Приказом 4-МР периодичность не устанавливает
2	ЕБС. Технологический участок обработки собранных биометрических персональных данных физических лиц с целью передачи в ЕБС	п.5 Приложения 3 Приказа Министерства цифрового развития, связи и массовых коммуникаций РФ от 25 июня 2018 г. N 321	2	Все кредитные организации	Вступило в силу	Ежегодно
3		п.2.3.2 Методические рекомендации Банка России от 14 февраля 2019 г. № 4-МР	2	Все кредитные организации	Вступило в силу	Не установлено
4		п.2.3.3 Методические рекомендации Банка России от 14 февраля 2019 г. № 4-МР	1	Системно значимые кредитные организации	Вступило в силу	Не установлено
5	Участок осуществления переводов денежных средств с использованием ССНП	п.3 Положения Банка России 672-П	2	Все кредитные организации	**Вступает в силу 1.07.2021** Не ниже 4 уровня к 1.01.2023	1 раз в 2 года
6	Участок осуществления переводов денежных средств с использованием СБП	п.4 Положения Банка России 672-П	2	Все кредитные организации	**Вступает в силу 1.07.2021** Не ниже 4 уровня к 1.01.2023	1 раз в 2 года
7	Автоматизированные системы и объекты среды обработки защищаемой информации (информации о переводах денежных средств)	п.3.1 Положения Банка России 683-П	2	Все кредитные организации	**Вступает в силу 1.01.2021** Не ниже 3 уровня к 1.01.2021 Не ниже 4 уровня к 1.01.2023	1 раз в 2 года
8			1	Системно значимые кредитные организации, кредитные организации, выполняющие функции оператора услуг платежной инфраструктуры системно значимых платежных систем, кредитные организации, значимые на рынке платежных услуг,	**Вступает в силу 1.01.2021** Не ниже 3 уровня к 1.01.2021 Не ниже 4 уровня к 1.01.2023	1 раз в 2 года
9	Автоматизированные системы и объекты среды обработки защищаемой информации (защищаемая информация в соответствии с п.1 Положения Банка России 684-П)	п.5.2 Положения Банка России 684-П	1	центральные контрагенты, центральный депозитарий	**Вступает в силу 1.01.2021** Не ниже 3 уровня к 1.01.2022 Не ниже 4 уровня к 1.01.2023	1 раз в год
10		п.5.3 Положения Банка России 684-П	2	Соответствующие критериям, описанным в п. 5.3 Положения	**Вступает в силу 1.01.2021** Не ниже 3 уровня к 1.01.2022 Не ниже 4 уровня к 1.07.2023	1 раз в 3 года
11		п.5 Положения Банка России 684-П	3	остальные	**Вступает в силу 1.01.2021**	Не установлено

Спасибо за внимание!
Вопросы?

Свинцицкий Антон Игоревич

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

http://www.DialogNauka.ru