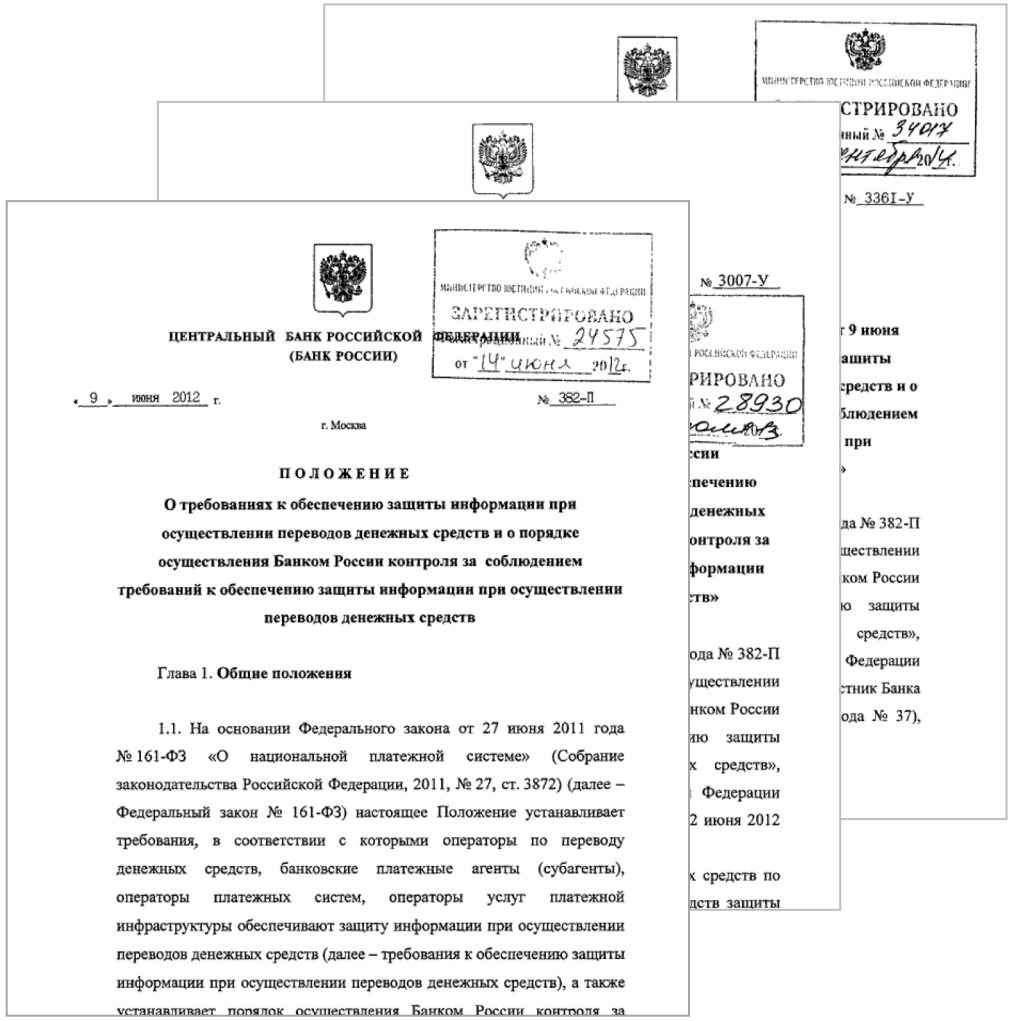
ОТ ПОЛОЖЕНИЯ БАНКА РОССИИ 382-П К ГОСТ Р 57580

Антон Свинцицкий
Директор по консалтингу
АО «ДиалогНаука»

ДиалогНаука

Положение Банка России 382-П



ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

ЗАРЕГИСТРИРОВАНО
от "14" июня 2012 г.

«9» июня 2012 г. № 382-П

г. Москва

П О Л О Ж Е Н И Е

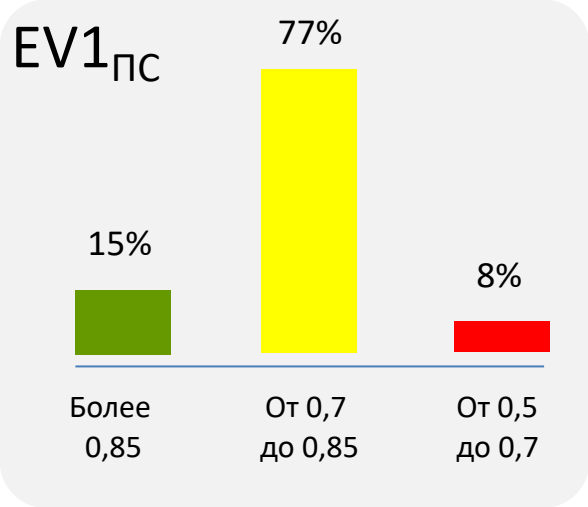
О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств

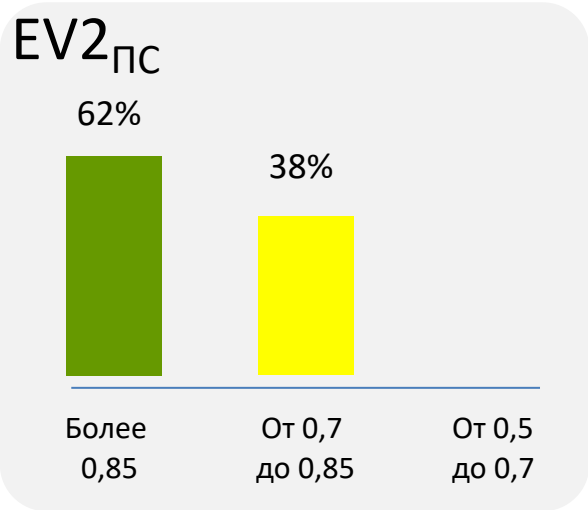
Глава 1. **Общие положения**

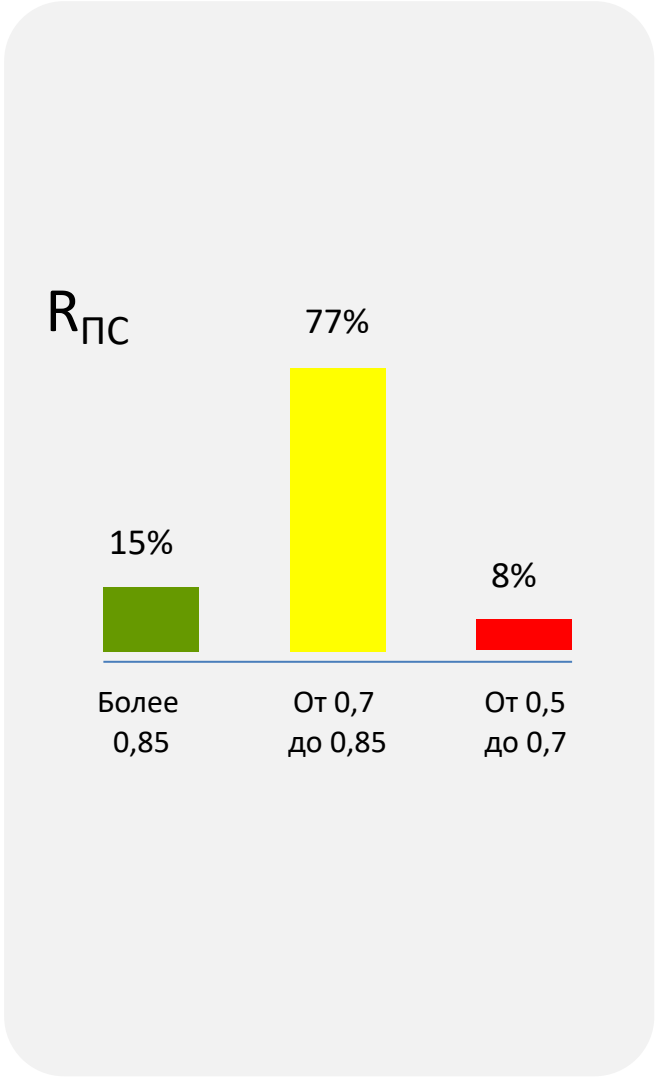
1.1. На основании Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе» (Собрание законодательства Российской Федерации, 2011, № 27, ст. 3872) (далее – Федеральный закон № 161-ФЗ) настоящее Положение устанавливает требования, в соответствии с которыми операторы по переводу денежных средств, банковские платежные агенты (субагенты), операторы платежных систем, операторы услуг платежной инфраструктуры обеспечивают защиту информации при осуществлении переводов денежных средств (далее – требования к обеспечению защиты информации при осуществлении переводов денежных средств), а также устанавливает порядок осуществления Банком России контроля за

Специалистами АО «ДиалогНаука» в период 2012-2018гг проведена оценка выполнения требования Положения 382-П в более чем 50 кредитных организациях

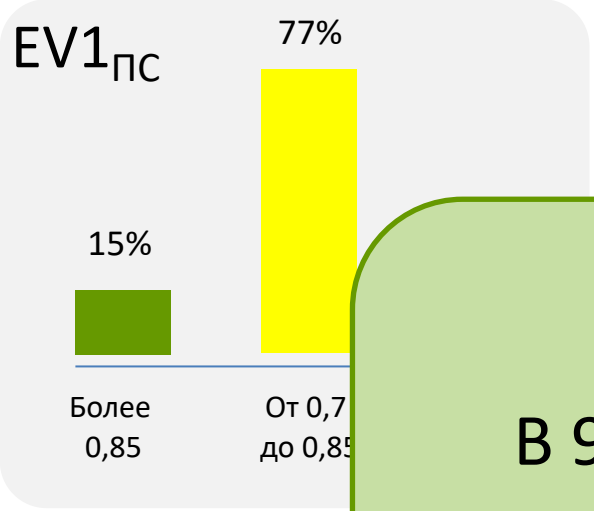
Обобщенные результаты оценки соответствия

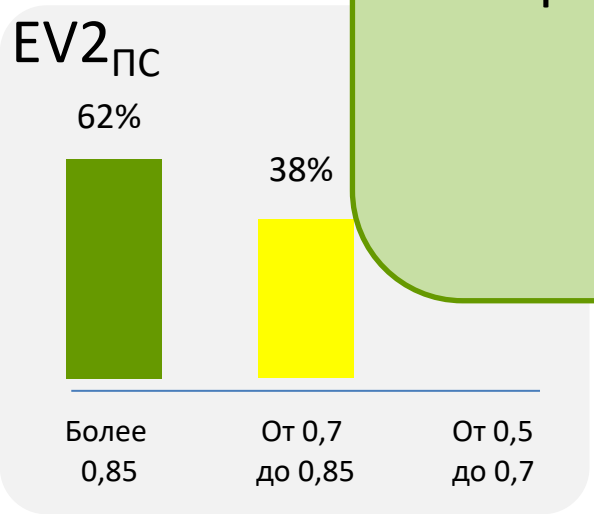






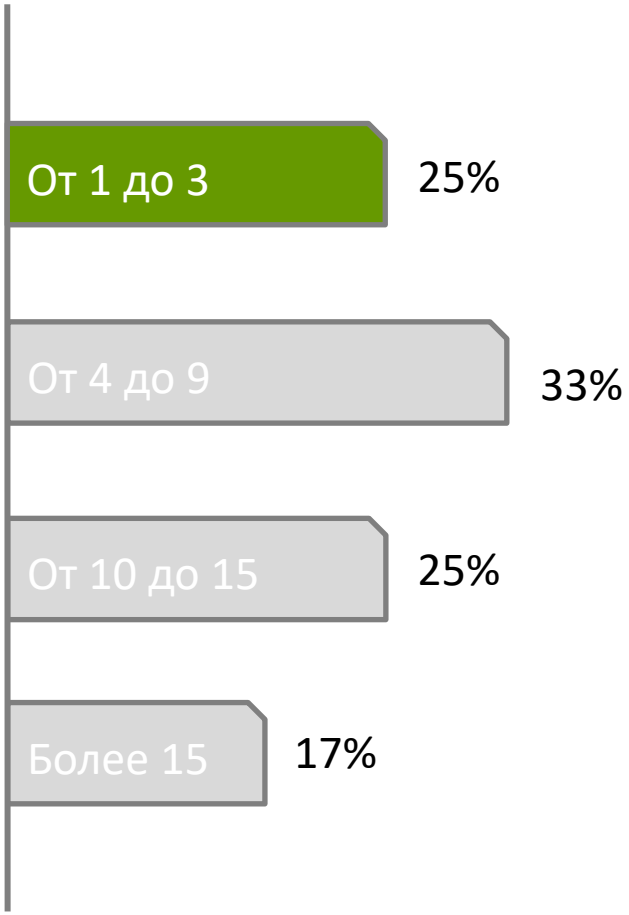
Обобщенные результаты оценки соответствия





В 93% проектов итоговая оценка $\mathbf{R_{ПС}}$ соответствовала оценке $\mathbf{EV1_{ПС}}$

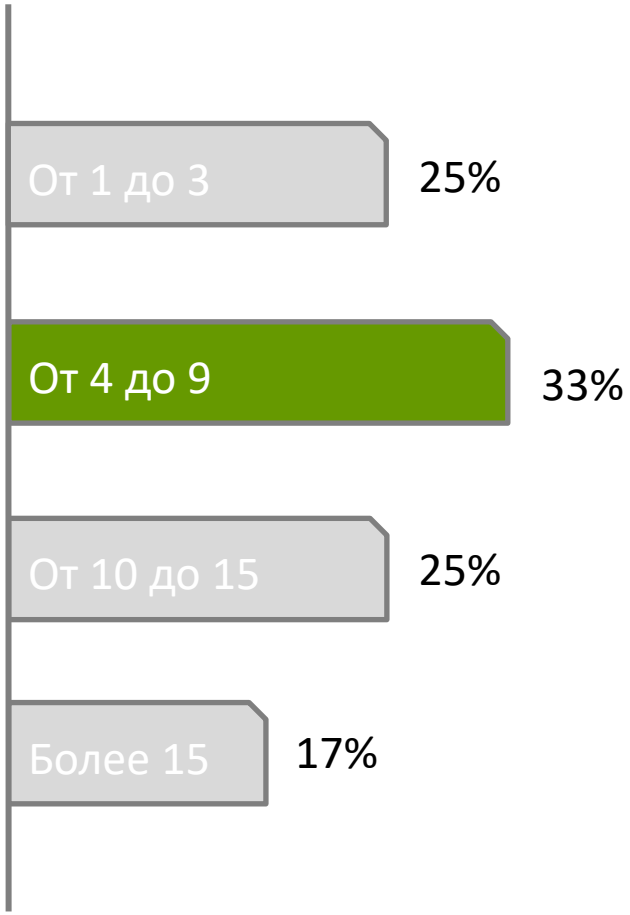
Кадровое обеспечение Службы ИБ



Решаемые задачи:

1. ~~Администрирование средств защиты информации~~
2. Разработка внутренних нормативных документов
3. Согласование доступа к информационным активам и объектам среды их обработки
4. ~~Мониторинг и контроль состояния ИБ~~
5. ~~Обеспечение ИБ на стадиях жизненного цикла АБС~~
6. ~~Управление рисками информационной безопасности~~
7. ~~Управление инцидентами ИБ~~
8. Выполнение требований законодательства РФ
9. СКЗИ
10. ~~Оценка эффективности~~

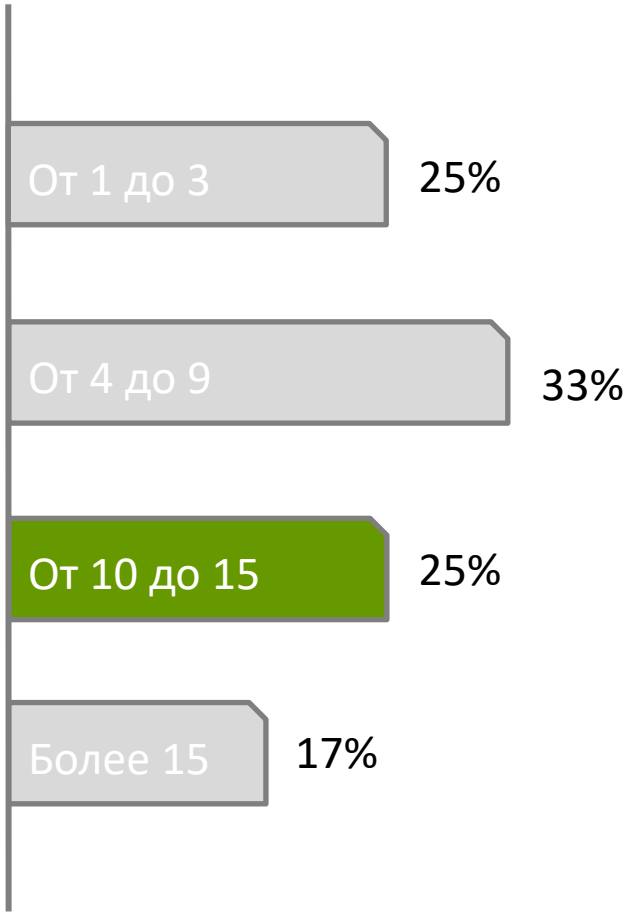
Кадровое обеспечение Службы ИБ



Решаемые задачи:

1. Администрирование средств защиты информации
2. Разработка внутренних нормативных документов
3. Согласование доступа к информационным активам и объектам среды их обработки
4. Мониторинг и контроль состояния ИБ
5. ~~Обеспечение ИБ на стадиях жизненного цикла АБС~~
6. ~~Управление рисками информационной безопасности~~
7. Управление инцидентами ИБ
8. Выполнение требований законодательства РФ
9. СКЗИ
10. ~~Оценка эффективности~~

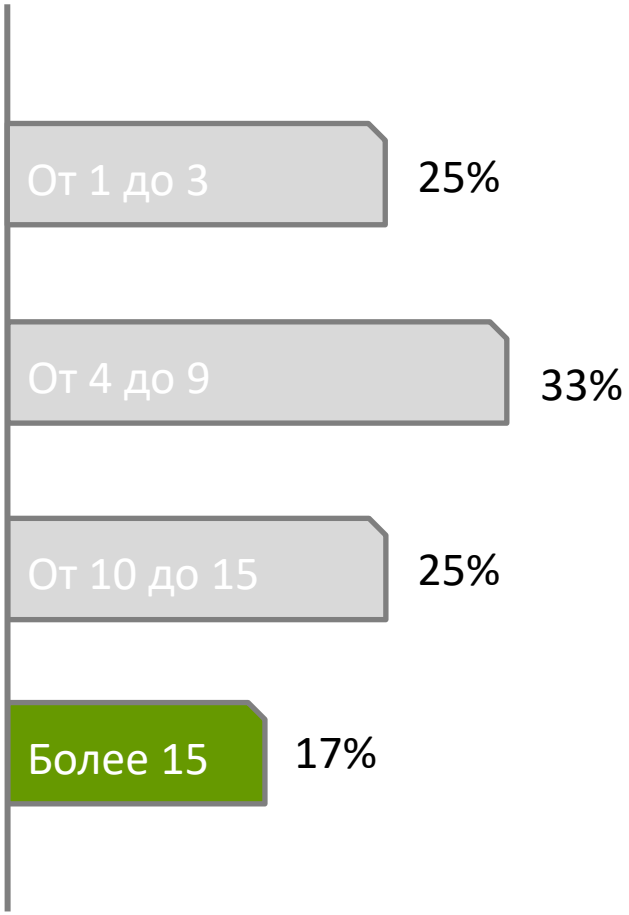
Кадровое обеспечение Службы ИБ



Решаемые задачи:

1. Администрирование средств защиты информации
2. Разработка внутренних нормативных документов
3. Согласование доступа к информационным активам и объектам среды их обработки
4. Мониторинг и контроль состояния ИБ
5. ~~Обеспечение ИБ на стадиях жизненного цикла АБС~~
6. ~~Управление рисками информационной безопасности~~
7. Управление инцидентами ИБ
8. Выполнение требований законодательства РФ
9. СКЗИ
10. ~~Оценка эффективности~~

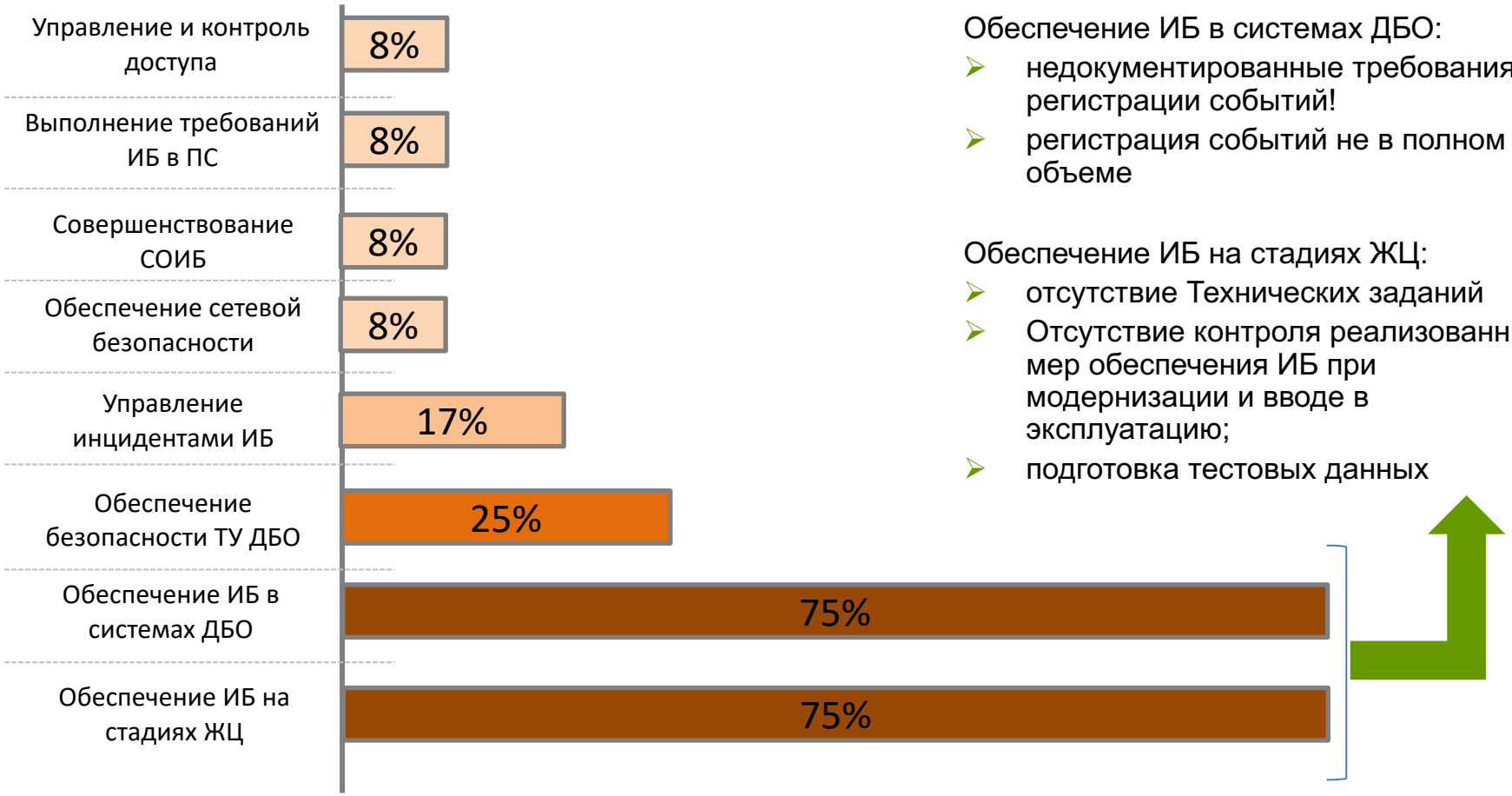
Кадровое обеспечение Службы ИБ



Решаемые задачи:

1. Администрирование средств защиты информации
2. Разработка внутренних нормативных документов
3. Согласование доступа к информационным активам и объектам среды их обработки
4. Мониторинг и контроль состояния ИБ
5. Обеспечение ИБ на стадиях жизненного цикла АБС
6. ~~Управление рисками информационной безопасности~~
7. Управление инцидентами ИБ
8. Выполнение требований законодательства РФ
9. СКЗИ
10. Оценка эффективности

Основные выявленные несоответствия по направлениям



Обеспечение ИБ в системах ДБО:

- недокументированные требования к регистрации событий!
- регистрация событий не в полном объеме

Обеспечение ИБ на стадиях ЖЦ:

- отсутствие Технических заданий
- Отсутствие контроля реализованных мер обеспечения ИБ при модернизации и вводе в эксплуатацию;
- подготовка тестовых данных

Основные выявленные несоответствия по направлениям

Обеспечение безопасности ТУ ДБО:

- маркировка;
- классификация;
- документирование процессов обеспечения ИБ;
- антивирусы

Управление инцидентами ИБ:

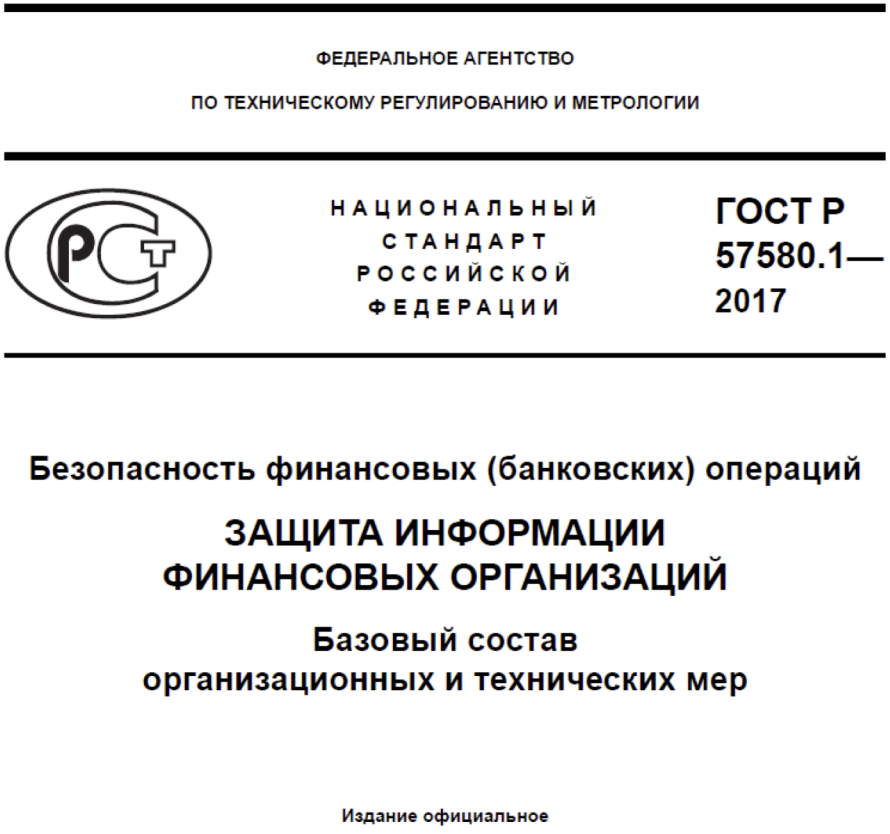
- отсутствие документации процесса;
- отсутствие свидетельств выполнения деятельности;
- отправка отчетности по инцидентам и результатам оценки соответствия (определенных в правилах ПС)

Немного фактов

- ✓ примерно 60% используются два и более различных вендора АВПО
- ✓ менее 50% используют или планируют использовать АВПО на банкоматах
- ✓ не более 25% используют DLP системы
- ✓ менее 25% в качестве межсетевых экранов используют ACL на сетевом оборудовании
- ✓ примерно 40% Заказчиков используют сертифицированные средства криптографической защиты для защиты каналов связи
- ✓ средства анализа защищенности используют около 60% Заказчиков
- ✓ тестирование на проникновение проводят менее 50% Заказчиков

- ✓ для 50% новых заказчиков оценка проводилась в первых раз в виде внешней оценки соответствия
- ✓ среднее улучшение оценки в двухлетний цикл составляет всего +0,05

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

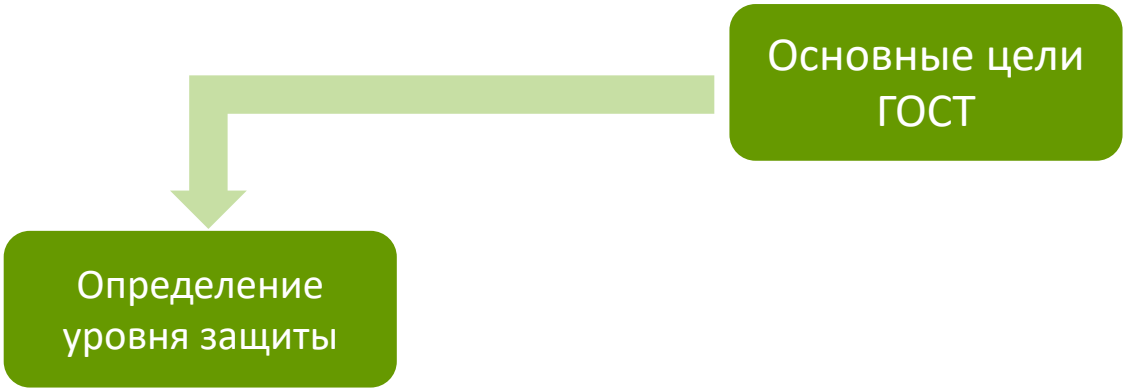
Издание официальное

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

Основные цели ГОСТ

ГОСТ Р 57580.1-2017



ГОСТ Р 57580.1-2017

ГОСТ Р 57580.1-2017

ГОСТ Р 57580.1-2017

ГОСТ Р 57580.1-2017

ГОСТ Р 57580.1-2017

ГОСТ Р 57580.1-2017

ГОСТ Р 57580.1-2017

Определение контуров безопасности

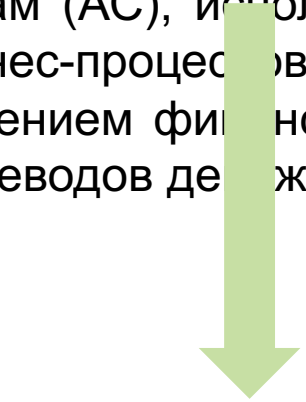
Цитата:

«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:

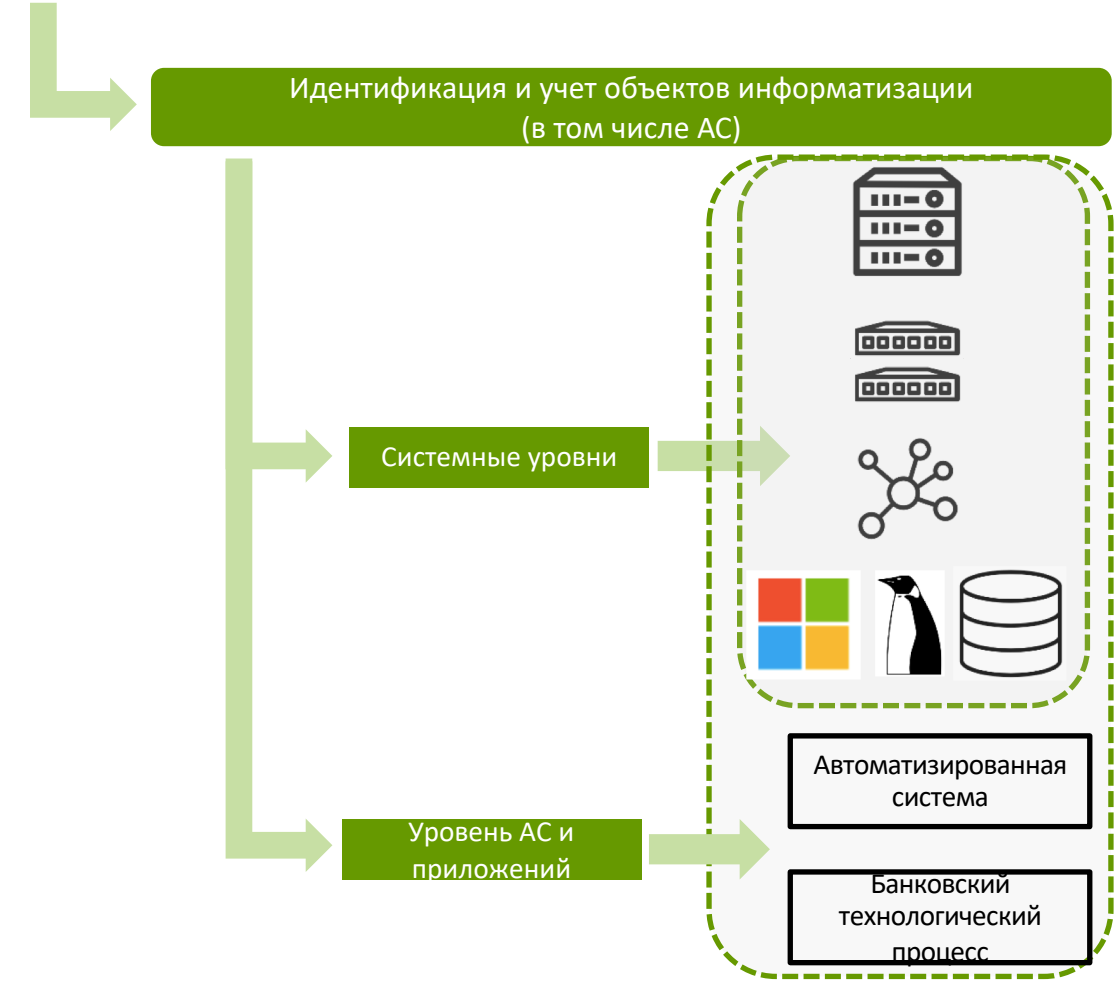
«Базовый состав мер защиты информации, определяемый настоящим стандартом, применим к совокупности объектов информатизации, в том числе автоматизированным системам (АС), используемым финансовыми организациями для выполнения бизнес-процессов и (или) технологических процессов, связанных с предоставлением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



Контуры безопасности

Определение контуров безопасности

- ✓ Уровень защиты информации определяется для контура безопасности



Определение контуров безопасности

СТО БР ИББС 1.0-2014

6.2. Деятельность организации БС РФ поддерживается входящей в ее состав информационной инфраструктурой, которая обеспечивает реализацию банковских технологий и может быть представлена в виде иерархии следующих основных уровней:

- физического (линии связи, аппаратные средства и пр.);
- сетевого оборудования (маршрутизаторы, коммутаторы, концентраторы и пр.);
- сетевых приложений и сервисов;
- операционных систем (ОС);
- систем управления базами данных (СУБД);
- банковских технологических процессов и приложений;
- бизнес-процессов организации.

8.3.3. Должны быть определены, выполняться, регистрироваться и контролироваться процедуры учета объектов среды для каждого информационного актива и (или) типа информационного актива, покрывающие все уровни информационной инфраструктуры организации БС РФ, определенной в разделе 6 настоящего стандарта.

ГОСТ 57580.1

6.2 При идентификации и учете объектов информатизации финансовой организации должны рассматриваться, как минимум, следующие основные уровни информационной инфраструктуры:

а) системные уровни:

- уровень аппаратного обеспечения;
- уровень сетевого оборудования;
- уровень сетевых приложений и сервисов;
- уровень серверных компонентов виртуализации, программных инфраструктурных сервисов;
- уровень операционных систем, систем управления базами данных, серверов приложений;

б) уровень АС и приложений, эксплуатируемых для оказания финансовых услуг в рамках бизнес-процессов или технологических процессов финансовой организации.

Определение контуров безопасности

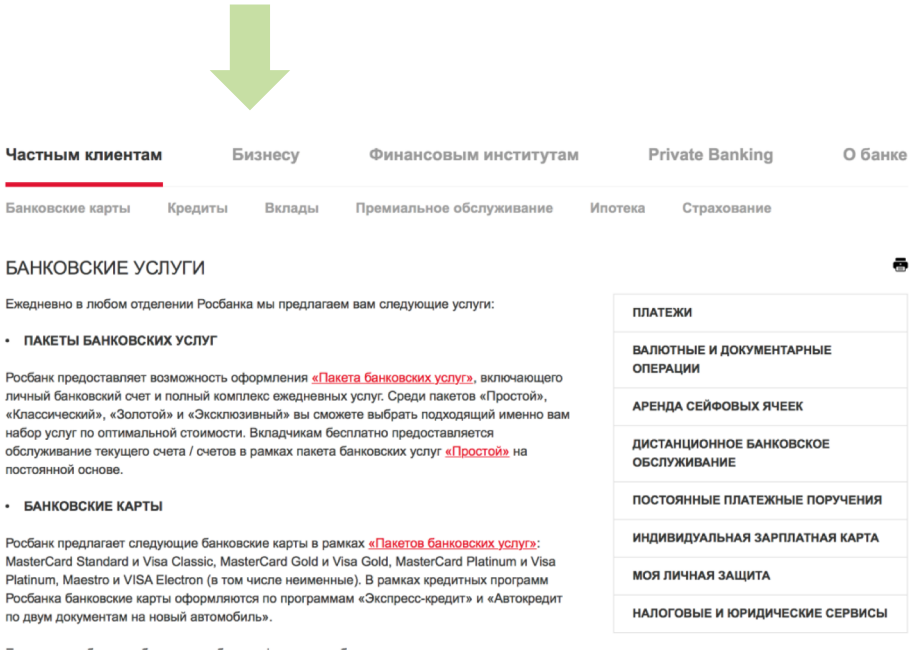
Цитата:

«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:

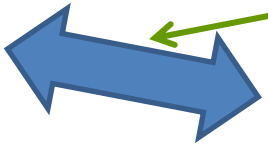
«Базовый состав мер защиты информации, определяемый настоящим стандартом, применим к совокупности объектов информатизации, в том числе автоматизированным системам (АС), используемым финансовыми организациями для выполнения бизнес-процессов и (или) технологических процессов, связанных с предоставлением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



Определение контуров безопасности

Осуществление переводов денежных средств

Клиент



Банк

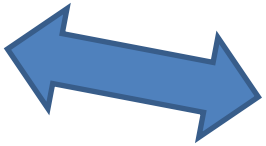
Автоматизированные банковские системы, обеспечивающие взаимодействие с клиентами Банка:

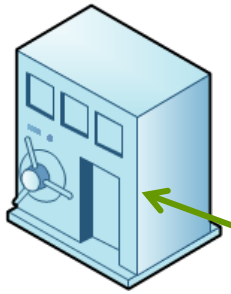
- удаленное взаимодействие (Системы ДБО)
- взаимодействие в отделениях Банка

Определение контуров безопасности

Осуществление переводов денежных средств

Клиент





Банк

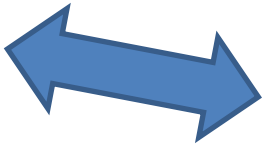
Автоматизированные банковские системы, обеспечивающие обработку платежной информации внутри Банка:

- АБС;
- Процессинговые системы

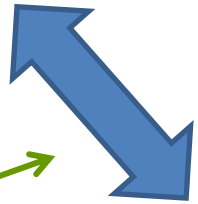
Определение контуров безопасности

Осуществление переводов денежных средств

Клиент



Банк



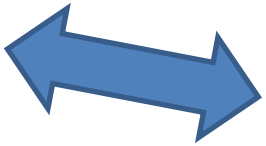
Автоматизированные банковские системы, обеспечивающие взаимодействие с платежными системами:

- АРМ КБР;
- SWIFT Alliance;
- Процессинговые системы

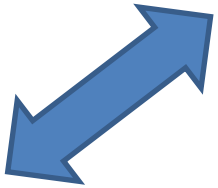
Определение контуров безопасности

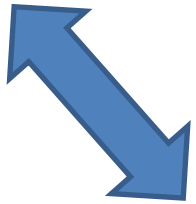
Осуществление переводов денежных средств

Клиент

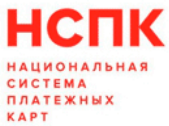


Банк





Банк



Определение уровней защиты информации

- ✓ Уровень защиты информации определяется для контура безопасности
- ✓ Факторы, влияющие на определение уровня защиты информации

Определение уровня защиты

- Минимальный
- Стандартный
- Усиленный

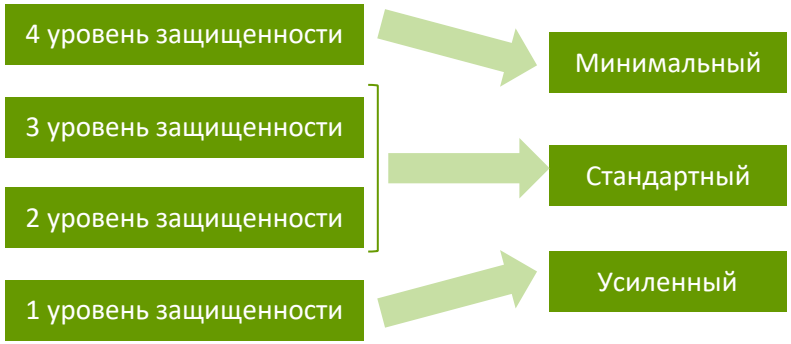
Банк России

Устанавливается нормативными актами Банк России

- ✓ Вид деятельности
- ✓ Состав финансовых услуг и реализуемых БТП
- ✓ Объем финансовых операций
- ✓ Размер организаций
- ✓ Значимость финансовой организации

Определение уровней защиты информации

- ✓ Уровень защиты информации определяется для контура безопасности
- ✓ Факторы, влияющие на определение уровня защиты информации
- ✓ Уровни защиты ПДн при их обработке в ИСПДн



В соответствии с Постановлением Правительства РФ ПП-1119

Базовые требования

Формирование политики обеспечения защиты информации финансовой организации, содержащей:

- ✓ цели и задачи защиты информации
- ✓ основные типы защищаемой информации
- ✓ основные принципы и приоритеты выбора организационных и технических мер системы защиты информации и системы организации и управления защитой информации;
- ✓ положения о выделении необходимых и достаточны ресурсов, используемых при применении организационных и технических мер, входящих в систему защиты информации.

Оглавление

ISO/IEC 27001:2013

5.2 Policy

Top management shall establish an information security policy that:

a) is appropriate to the purpose of the organization;

b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives;

c) includes a commitment to satisfy applicable requirements related to information security; and

d) includes a commitment to continual improvement of the information security management system.

Базовые требования

Базовые требования

- Обеспечение целостности
- Обеспечение доступности
- Защита сред виртуализации
- Защита технических средств
- Выявление инцидентов
- Управление конфигурацией

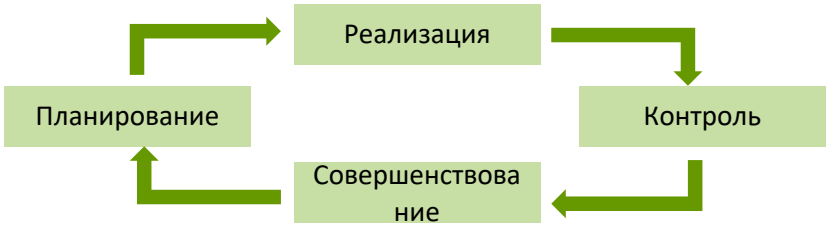
?

Базовые требования

Требования к системе защиты информации

- Обеспечение ЗИ при управлении доступом
- Контроль целостности
- Предотвращение утечек
- Защита сред виртуализации
- Обеспечение защиты вычислительных сетей
- Защита от вредоносного кода
- Управление инцидентами ЗИ
- Удаленный доступ и мобильные устройства

Требования к организации и управлению защитой информации



- Требования к защите информации на этапах ЖЦ
- Рекомендации по защите ПДн

?

- Идентификация и аутентификация субъектов доступа и объектов доступа
- Управление доступом субъектов доступа к объектам доступа
- Защита машинных носителей информации
- Регистрация событий
- Антивирусная защита
- Обнаружение вторжений
- Контроль и анализ защищенности

Приказ ФСТЭК России №21

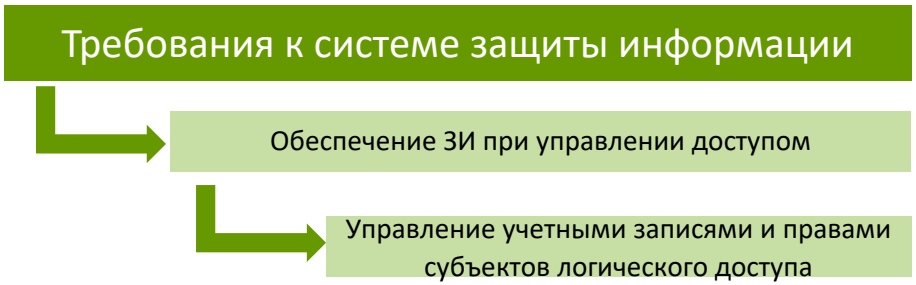
Базовые требования

Требования к системе защиты информации

Обеспечение ЗИ при управлении доступом

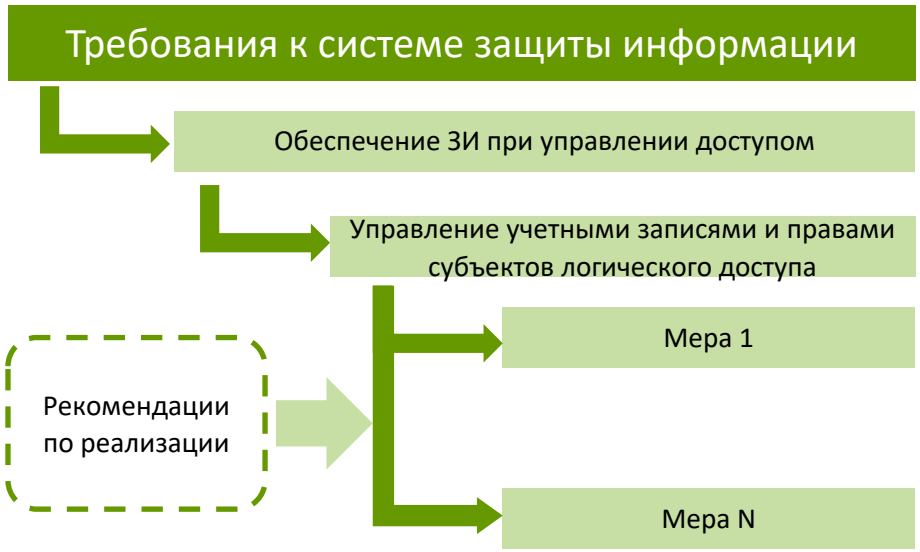
Направление	3 направления
Процесс	8 процессов

Базовые требования



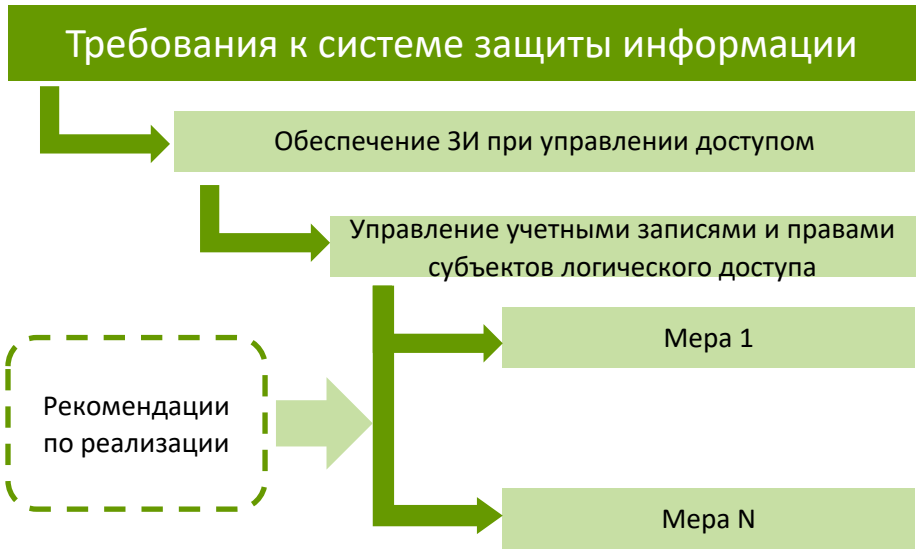
Направление	3 направления
Процесс	8 процессов
Подпроцесс	

Базовые требования



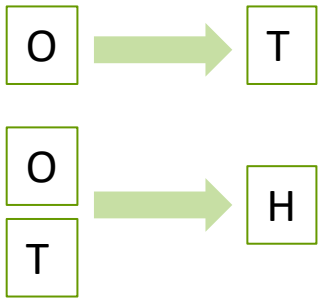
Направление	3 направления
Процесс	8 процессов
Подпроцесс	
Меры системы защиты информации	408 мер (на самом деле 667!)

Базовые требования



Направление	3 направления
Процесс	8 процессов
Подпроцесс	
Меры системы защиты информации	408 мер (на самом деле 667!)

Примечание:

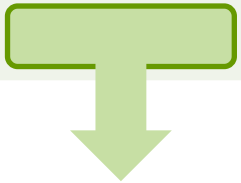


Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
УЗП.5	Документарное определение правил предоставления (отзыва) и блокирования логического доступа	Н	О	О
УЗП.6	Назначение для всех ресурсов доступа распорядителя логического доступа (владельца 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

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

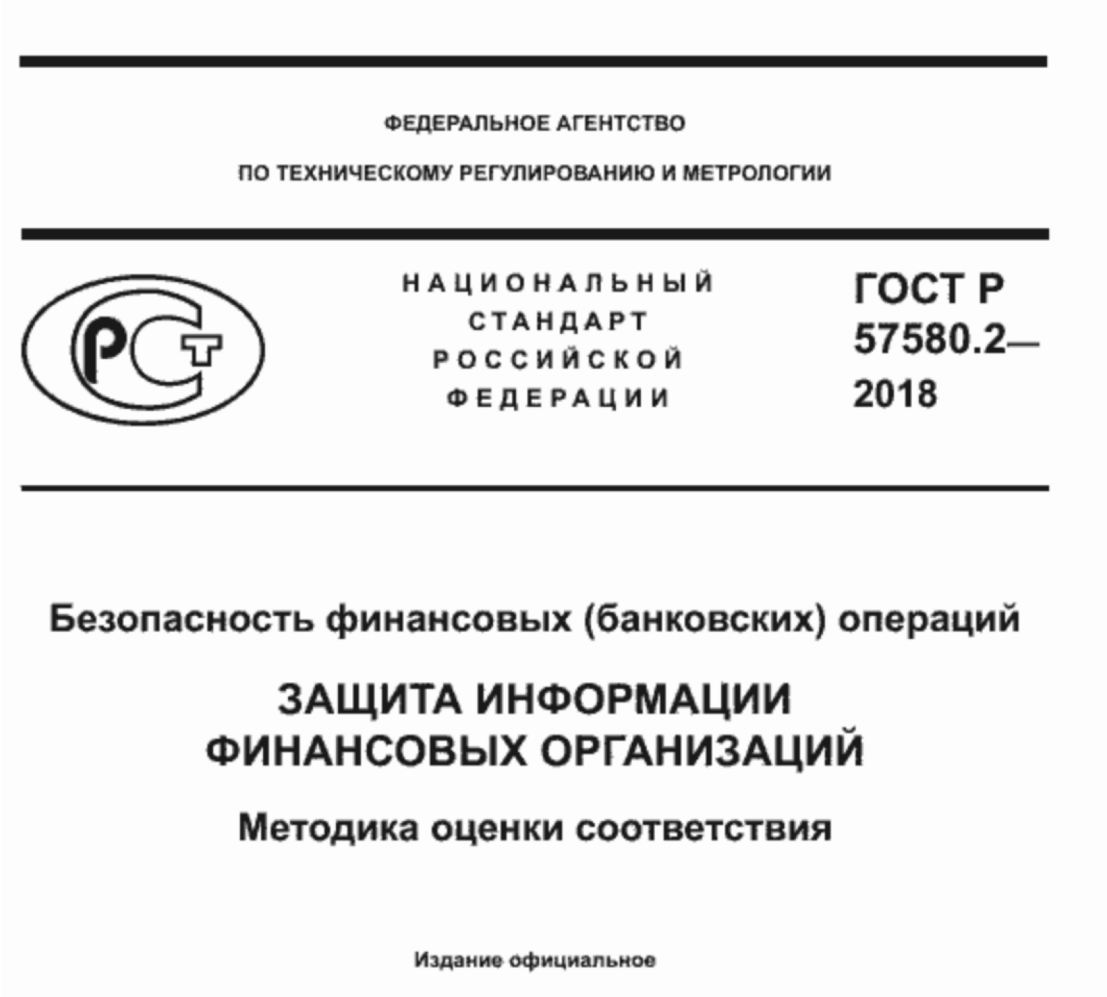
Условное обозначение и номер меры	Применение меры на уровнях среды обработки				
	Аппаратное обеспечение	Сетевое оборудование	ОС	СУБД	…



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…

Методика оценка соответствия



ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 57580.2— 2018

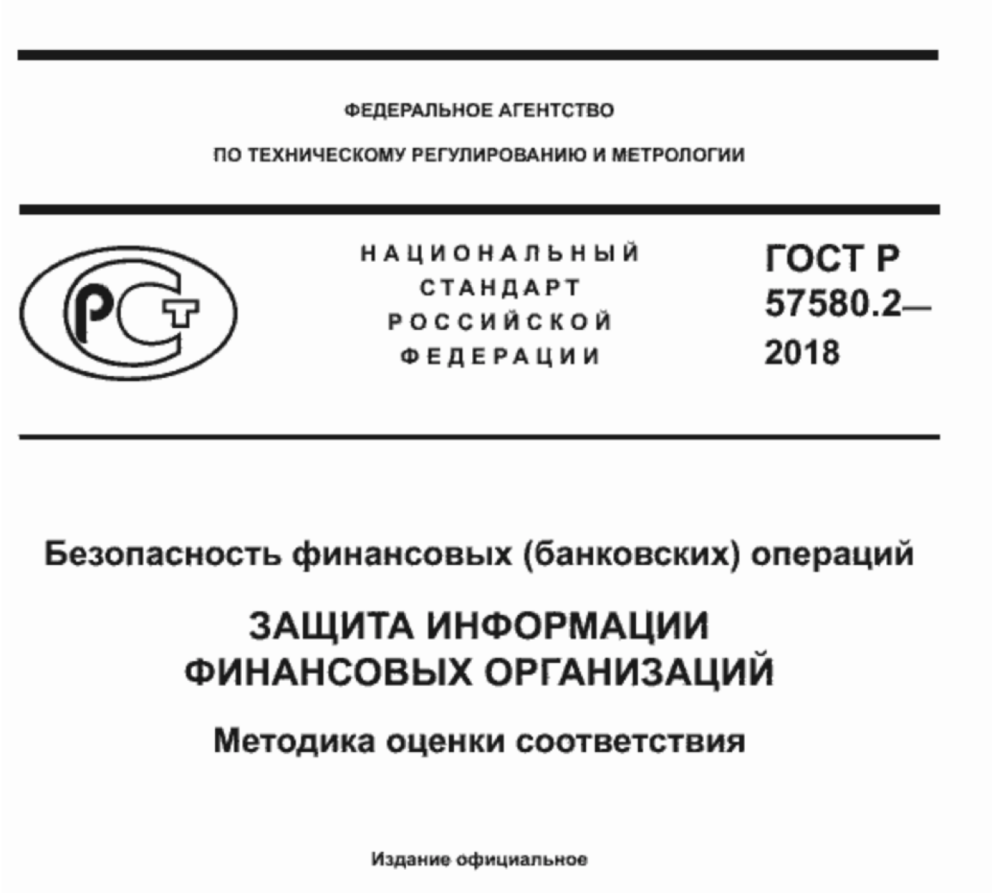
Безопасность финансовых (банковских) операций

ЗАЩИТА ИНФОРМАЦИИ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

Методика оценки соответствия

Издание официальное

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

ГОСТ вводится в действие с **1.01.2018**

(носит рекомендательный характер, как любой ГОСТ на территории Российской Федерации)

- ✓Положения Банка России устанавливающие статус ГОСТа (проект Положения Банка России)
- ✓Методика выбора уровня защиты (проект Положения Банка России, Приказ Минцифры)

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)

Методика оценки соответствия

- ✓ Для оценки полноты реализации процессов системы ЗИ используется следующая качественная модель оценивания

Уровни соответствия

- Нулевой уровень соответствия
- Первый уровень соответствия
- Второй уровень соответствия
- Третий уровень соответствия
- Четвертый уровень соответствия
- Пятый уровень соответствия

Уровни зрелости процесса

- 0 Отсутствующий. Процесс не существует. Например, процесс производства колбасы в ИТ организации находится на нулевом уровне зрелости, поскольку мы не производим колбасу.
- 1 Начальный. Деятельность осуществляется хаотически, от случая к случаю без единого подхода. Руководство не организовано.
- 2 Повторяемый, но интуитивный. Одинаковые задачи решаются разными людьми сходными методами. Однако отсутствуют формальные процедуры и распределение ответственности. Весьма высока зависимость от отдельных сотрудников, что повышает вероятность ошибок.
- 3 Определенный. Процедуры стандартизованы и документированы. Однако отклонения от процедур не всегда отслеживаются. Процедуры формализуют существующую практику.
- 4 Управляемый и измеримый. Руководство контролирует и измеряет процесс и принимает меры, если процесс неэффективен. Могут использоваться инструменты автоматизации процесса.
- 5 Оптимизируемый. Процесс развит до уровня хорошей практики в результате постоянных улучшений и сравнения с другими предприятиями. Соответствует целям заказчика. Сравните рассмотренные выше этапы развития процесса. Они суть уровни зрелости. Таким образом, развивая процесс, мы последовательно поднимаем его уровень зрелости. Как определить на каком уровне он находится сейчас?

Схема оценки

Шаг 1.

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

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 (методика проверки модели угроз?)
   - ✓ добавление в реестр оценки компенсирующих мер (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

$$Е_{ППЗИ_i} = \frac{\sum_{j=1}^{N} E_{МЗИ_j}}{N}$$

$$Е_{ПЗИ_i} = \frac{\sum_{k=1}^{T} E_{ППЗИ_K}}{T}$$

Применимо для процессов 1,2 и 6

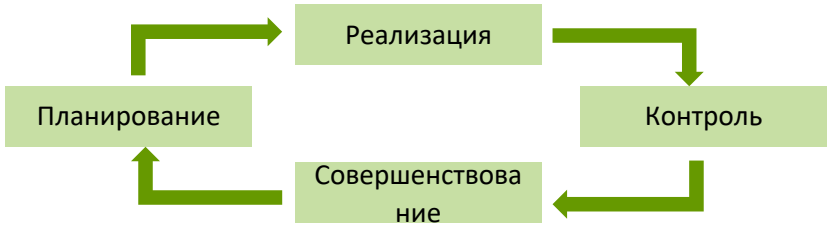
$$Е_{ПЗИ_i} = \frac{\sum_{j=1}^{N} E_{МЗИ_j}}{N}$$

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

- ✓ Для уровня ЗИ = 3 $Е_{ППЗИ} = \frac{\sum_{j=1}^{22} E_{МЗИ_j}}{22}$
- ✓ Для уровня ЗИ = 2 $Е_{ППЗИ} = \frac{\sum_{j=1}^{27} E_{МЗИ_j}}{27}$

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***

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

Перечень нарушений

Выявленное нарушение	Процесс защиты информации							
	1	2	3	4	5	6	7	8
Осуществление логического доступа под учетными записями неопределенного целевого назначения	+							
Осуществление логического доступа под коллективными неперсонифицированными учетными записями	+							+
Наличие незаблокированных учетных записей уволенных работников	+							+
Отсутствие разграничения логического доступа	+							
Несанкционированное предоставление пользователям административных прав	+							
Несанкционированное предоставление пользователям прав логического доступа	+							+
Хранение паролей субъектов доступа в открытом виде	+							
Передача аутентификационных данных в открытом виде по каналам и линиям связи	+							+
Отсутствие регистрации персонификации, выдачи (передачи) и уничтожения персональных технических устройств аутентификации	+							
Отсутствие разграничения физического доступа в помещения, в которых расположены объекты доступа	+							
Несанкционированный физический доступ посторонних лиц в помещения, в которых расположены объекты доступа	+							

Перечень нарушений

Выявленное нарушение	Процесс защиты информации							
	1	2	3	4	5	6	7	8
Отсутствие сетевой изоляции внутренних вычислительных сетей финансовой организации и сети Интернет и (или) беспроводных сетей		+						
Передача информации конфиденциального характера с использованием сети Интернет, телекоммуникационных каналов и (или) линий связи, не контролируемых финансовой организацией, в открытом виде					+			
Наличие в контролируемой зоне финансовой организации незарегистрированных точек беспроводного доступа, имеющих подключение к ЛВС финансовой организации		+						
Использование нелицензионного ПО								
Отсутствие применения средств защиты от воздействия вредоносного кода				+				
Обработка информации конфиденциального характера с использованием неучтенных МНИ					+			
Отсутствие гарантированного стирания информации конфиденциального характера с МНИ при осуществлении их вывода из эксплуатации или вывода из эксплуатации СВТ, в состав которой входят указанные МНИ, а также при необходимости их передачи в сторонние организации					+			
Отсутствие реагирования на инциденты ЗИ							+	

Требования к отчетным документам

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

СТО БР ИББС

- ✓ сведения об аудиторской организации
- ✓ сведения о руководителе и членах аудиторской группы
- ✓ сведения о проверяемой организации
- ✓ сведения о заказчике аудита ИБ
- ✓ цель аудита ИБ
- ✓ область аудита ИБ, в частности, сведения о проверенных организационных и функциональных единицах или процессах и охваченном периоде времени
- ✓ сроки проведения аудита ИБ
- ✓ план аудита ИБ на месте
- ✓ документально оформленную совокупность анкет, содержащих критерии аудита ИБ и выводы аудита ИБ, сделанные по каждому из рассмотренных критериев аудита ИБ
- ✓ заключение по результатам аудита ИБ
- ✓ перечень представителей со стороны проверяемой организации, которые сопровождали и опрашивались аудиторской группой при проведении аудита ИБ
- ✓ краткое изложение процесса аудита ИБ, включая элемент неопределенности и/или проблемы, которые могут отразиться на надежности заключения по результатам аудита ИБ;
- ✓ подтверждение, что цель аудита ИБ достигнута в области аудита ИБ в соответствии с планом аудита ИБ
- ✓ любые неохваченные области, входящие в область аудита ИБ
- ✓ любые неразрешенные разногласия между аудиторской группой и проверяемой организацией
- ✓ заявление о конфиденциальном характере содержания отчета
- ✓ лист рассылки отчета по результатам аудита ИБ

Требования к отчетным документам

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

СТО БР ИББС

- ✓ сведения об аудиторской организации
- ✓ сведения о руководителе и членах аудиторской группы
- ✓ сведения о проверяемой организации
- ✓ сведения о заказчике аудита ИБ
- ✓ цель аудита ИБ
- ✓ область аудита ИБ, в частности, сведения о проверенных организационных и функциональных единицах или процессах и охваченном периоде времени
- ✓ сроки проведения аудита ИБ
- ✓ план аудита ИБ на месте
- ✓ документально оформленную совокупность анкет, содержащих критерии аудита ИБ и выводы аудита ИБ, сделанные по каждому из рассмотренных критериев аудита ИБ
- ✓ заключение по результатам аудита ИБ
- ✓ перечень представителей со стороны проверяемой организации, которые сопровождали и опрашивались аудиторской группой при проведении аудита ИБ
- ✓ краткое изложение процесса аудита ИБ, включая элемент неопределенности и/или проблемы, которые могут отразиться на надежности заключения по результатам аудита ИБ;
- ✓ подтверждение, что цель аудита ИБ достигнута в области аудита ИБ в соответствии с планом аудита ИБ
- ✓ любые неохваченные области, входящие в область аудита ИБ
- ✓ любые неразрешенные разногласия между аудиторской группой и проверяемой организацией
- ✓ заявление о конфиденциальном характере содержания отчета
- ✓ лист рассылки отчета по результатам аудита ИБ

Требования к отчетным документам

В заключении:

Отчет по результатам оценки соответствия ЗИ должен быть **прошит** и **скреплен мастичной печатью** проверяющей организации с указанием количества листов в заверительной надписи, подписанной руководителем проверяющей группы.

Для каждого электронного документа, файла данных, прилагаемых к отчету по результатам оценки соответствия ЗИ, **должны быть вычислены хэш-функции, реализованной в соответствии с ГОСТ Р 34.11-2012**

Спасибо за внимание!
Вопросы?

АО «ДиалогНаука»
Телефон: +7 (495) 980-67-76
Факс: +7 (495) 980-67-75

http://www.DialogNauka.ru