ПОСТРОЕНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ ГОСТ Р 57580.1-2017. ОЦЕНКА СООТВЕТСТВИЯ.

Ксения Засецкая
Старший консультант
АО «ДиалогНаука»

Москва, 28 апреля 2020 года

ДиалогНаука

План вебинара

В рамках вебинара будут рассмотрены следующие темы:

- ✓ Выполнение требований нормативных документов Банка России.
- ✓ ГОСТ Р 57580.1-2017 как основной «инструмент» для определения требований к процессам и подсистемам защиты информации.
- ✓ ГОСТ Р 57580.1. Цели. Задачи. Подходы.
- ✓ Проведение оценки соответствия. ГОСТ Р 57580.2-2018. Методика оценки. Этапы работ. Требования к формирования отчетных материалов.

Нормативные документы Банка России

- ✓ Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента от 17 апреля 2019 г. N 683-П
- ✓ О требованиях к защите информации в платежной системе Банка России от 9 января 2019 г. N 672-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 от 9 июня 2012 г. N 382-П
- ✓ Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций от 17 апреля 2019 г. № 684-П

- ✓ статья 6, п.4 кредитные организации обязаны направлять с 1 июля 2020 года в Банк России сведения:
  - ✓ 1) о поставщиках платежных приложений для включения их в перечень поставщиков платежных приложений;
  - ✓ 2) о БПА, осуществляющих деятельность платежных агрегаторов, для включения их в перечень банковских платежных агентов, осуществляющих деятельность платежных агрегаторов.

- ✓ Расширен круг субъектов НПС:
  - ✓ платежные агрегаторы (ПА),
  - ✓ поставщики платежного приложения (ППП)

- ✓ Дополнительно по 264-ФЗ от 02.08.2019:
  - ✓ операторы услуг информационного обмена (ОУИО)
  - ✓ иностранный поставщик платежных услуг

382-П.Что нового с 01.01.2020

2.5.5.1¤	Оператору по переводу денежных с тору услуг платежной инфраструкту создания и эксплуатации объектов ной инфраструктуры необходимо о пользование для осуществления пер ных средств прикладного программ ния автоматизированных систем и сертифицированных в системе серт деральной службы по техническому контролю на соответствие требова опасности информации, включая анализу уязвимостей и контролю от кларированных возможностей, в соот конод ноше треб же че Р ИС
2.10.5¤	При осуществлении переводов денежных средств с использованием сети Интернет и (или) размещении программного обеспечения, используемого клиентом при осуществлении переводов денежных средств, на средствах вычислительной техники, для которых оператором по переводу денежных средств не обеспечивается непосредственный контроль защиты информации от воздействия вредоносного кода, оператору по переводу денежных средств необходимо обеспечить реализацию технологических мер по использованию раздельных технологий и (или) реализовать ограничения по параметрам операций по осуществлению переводов денежных средств определяемых договором опе денежных средств с клиентом, возможность установления ука й по инициативе клиента¶
2.10.6¤	Реализуемые оператором по переводу денежных средств технологические меры по использованию раздельных технологий должны обеспечивать:¶ идентификацию и аутентификацию клиента при подготовке клиентом и при подтверждении клиентом электронных сообщений;¶ возможность использования клиентом независимых программных сред для подготовки и подтверждения электронных сообщений;¶ возможность контроля клиентом реквизитов распоряжений о переводе денежных средств при подготовке электронных сообщений (пакета электронных сообщений) и их подтверждении;¶ аутентификацию входных электронных сообщений (пакета электронных сообщений) путем использования и сравнения (сверки) аутентификационных данных, сформированных на основе информации о реквизитах распоряжений о переводе денежных средств при подготовке клиентом электронных сообщений (пакета электронных сообщений) и подтверждении клиентом электронных сообщений;¶ удостоверение оператором по переводу денежных средств распоряжений о переводе денежных

382-П. Проект изменений

- ✓ Вступление в силу новых требований – 01.01.2023 (в проекте)
- ✓ Исключается Приложение 1 “Порядок проведения оценки соответствия и документирования ее результатов”,
- ✓ К 14.1 будет добавлено требование проведения оценки соответствия уровням защиты информации в соответствии с национальным стандартом Российской Федерации ГОСТ Р 57580.2-2018
- ✓ Представлен перечень из 11 технологических мер для обеспечения защиты информации при осуществлении переводов денежных средств
- ✓ Учтено, на каких технологических участках меры требуется применять
- ✓ Платежные агрегаторы , поставщики платежного приложения, операторы услуг информационного обмена

уровень соответствия – не ниже четвертого – к 01.01.2023

382-П. Проект изменений

- ✓ ГОСТ Р 57580.1-2017
- ✓ ОПДС, БПА, ОУИО, ОУПИ - реализация уровней защиты информации, определенных ГОСТ Р 57580.1-2017
- ✓ Ссылки Положение Банка России от 17.04.2019 № 683-П.
- ✓ ОПДС - обеспечение контроля за соблюдением БПА требований к обеспечению ЗИ
- ✓ ОПДС должны передавать в БР сведения по инцидентам, полученные от БПА (субагентов) - договор

Обеспечение с 01.01.2021 реализации требований ГОСТ Р 57580.1-2017:

- ✓ системно значимые КО - усиленный уровень (уровень 1) защиты информации по ГОСТ Р 57580.1-2017;
- ✓ остальные КО - стандартный уровень (уровень 2) защиты информации ГОСТ Р 57580.1-2017.

Требования к технологии обработки защищаемой информации

- ✓ на технологическом участке формирования (подготовки), передачи и приема электронных сообщений;
- ✓ на технологическом участке удостоверения прав клиентов распоряжаться денежными средствами;
- ✓ на технологическом участке осуществления банковской операции, учета результатов ее осуществления

Привлечение лицензиата!

- Сертификация прикладного ПО АС и приложений, распространяемых кредитной организацией клиентам для совершения действий в целях осуществления банковских операций, а также ПО, обрабатывающего защищаемую информацию на участках, используемых для приема электронных сообщений
- Требования к защите электронных сообщений на различных технологических участках обработки:
  - идентификация, аутентификация и авторизация клиентов при совершении действий в целях осуществления банковских операций;
  - формирование (подготовка), передача и прием электронных сообщений;
  - удостоверение права клиентов распоряжаться денежными средствами;
  - осуществление банковской операции, учет результатов ее осуществления;
  - хранение электронных сообщений и информации об осуществленных банковских операциях

Часть требований – с 01.07.2021

ПС БР

Участники ССНП

Участники СБП

ОПКЦ

Документирование

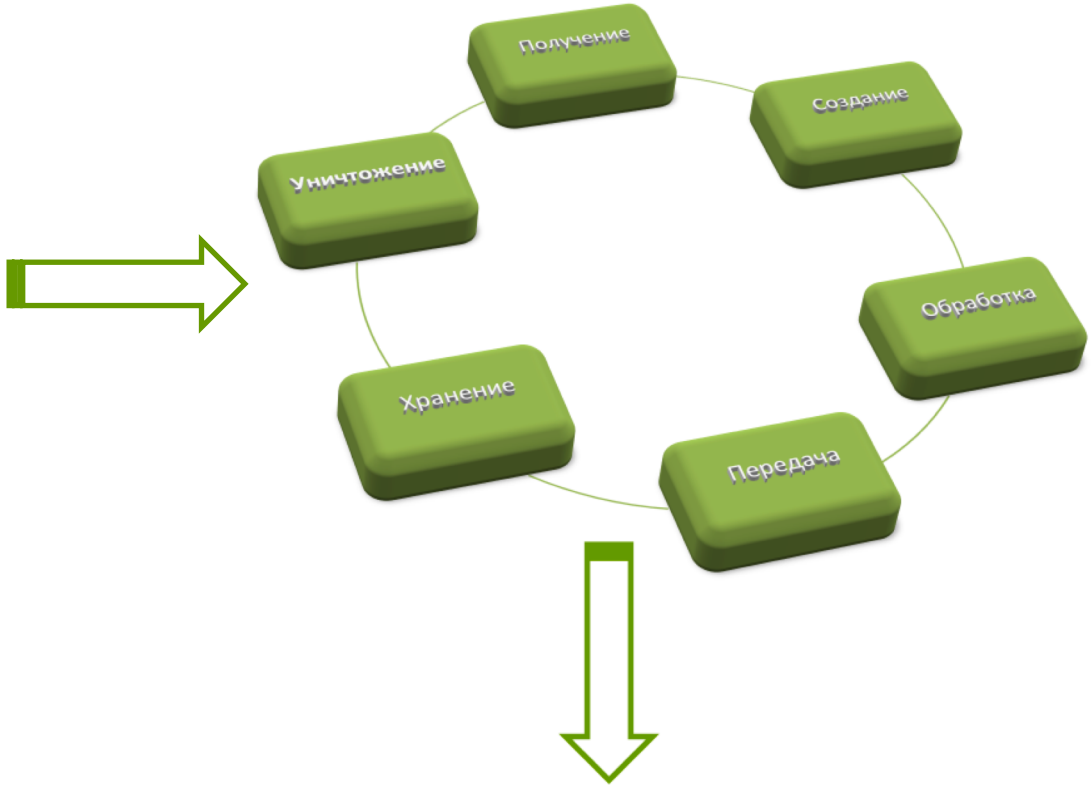
Защита электронных сообщений

Применение СКЗИ

Защищаемая информация

1. Электронные сообщения, формируемые работниками и клиентами НФО
2. Информация, необходимая для авторизации клиентов НФО при осуществлении операций
3. Информация о финансовых операциях НФО и клиентов
4. Ключевая информация СКЗИ

на всех стадиях ее жизненного цикла



в автоматизированных системах НФО,

а так же на объектах среды обработки защищаемой информации

Базовые требования к НФО

- ✓ **Информирование клиентов** о рисках информационно безопасности

- ✓ **Использование СКЗИ** в соответствии с:
  - законодательством Российской Федерации;
  - нормативными документами ФСБ России;
  - технической документации

- ✓ **Выполнение требований ГОСТ Р 57580.1-2017**

Определение уровня защиты

центральные контрагенты, центральный депозитарий	Усиленный
соответствующие критериям, описанным в п.5.3	Стандартный
остальные некредитные финансовые организации	Минимальный

Примечание: пересмотр применимого уровня защиты ежегодно не позднее первого рабочего дня календарного года

Сроки

06.04.2019
Вступил в силу 672-П

26.05.2019
Вступили в силу 684-П, 683-П

01.01.2020
Необходимость сертификации прикладного ПО АС

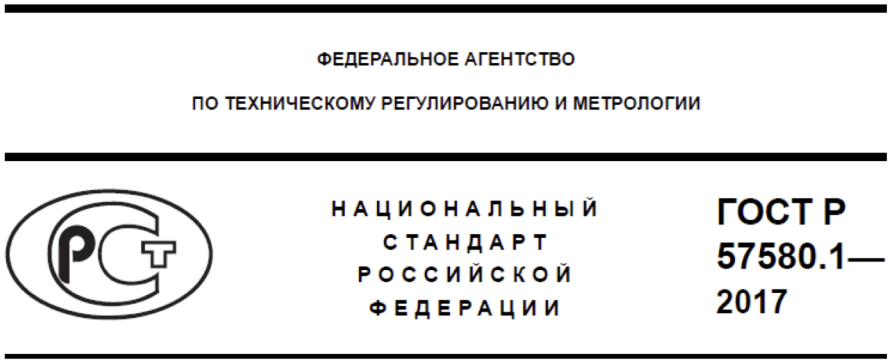
01.01.2021
1. Необходимость выполнения требований ГОСТ Р 57580.1-2017
2. Проведение тестирований на проникновение
3. Проведение оценки соответствия

01.07.2021
Дополнительные требования 672-П

01.01.2022
Необходимость обеспечения не ниже 3 уровня соответствия ГОСТ Р 57580.1-2017

01.07.2023
Необходимость обеспечения не ниже 4 уровня соответствия ГОСТ Р 57580.1-2017

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

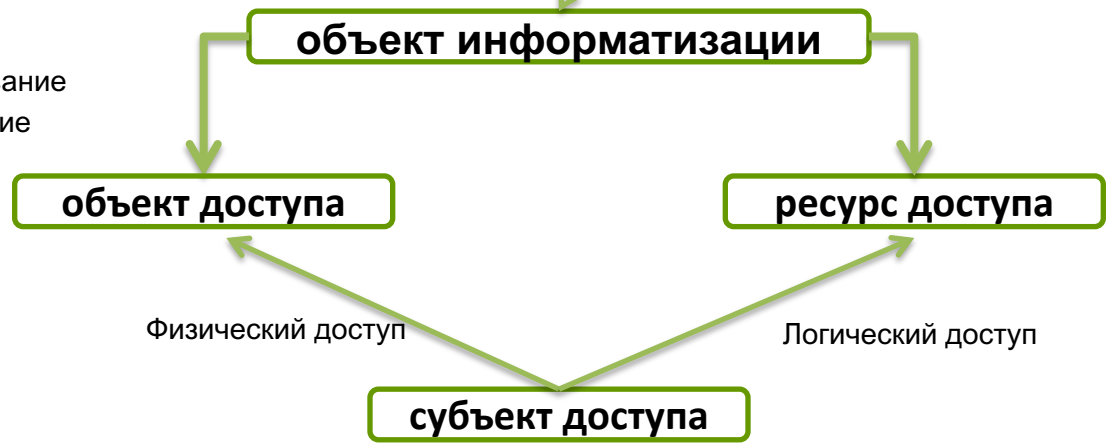
ГОСТ Р 57580.1-2017

ГОСТ Р 57580.1-2017

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

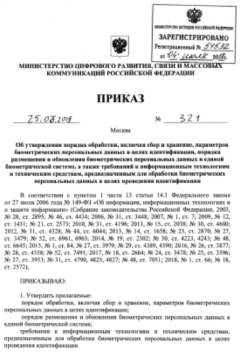
Определение контуров безопасности

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

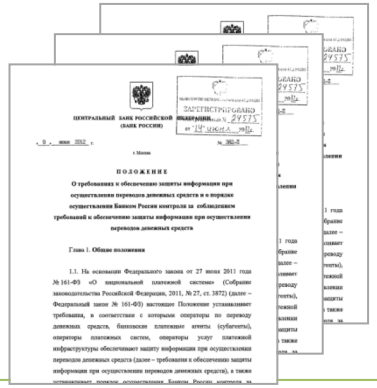
ПРИКАЗ

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

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

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».

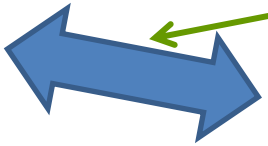
Единая степень критичности
Единая политика защиты информации

Контур безопасности

Определение контуров безопасности

Осуществление переводов денежных средств

Клиент



Банк

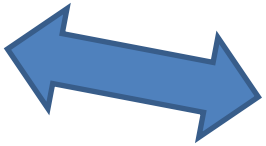
Автоматизированные банковские системы, обеспечивающие взаимодействие с клиентами Банка:

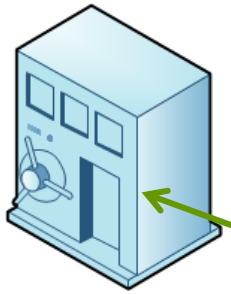
- удаленное взаимодействие (Системы ДБО)
- взаимодействие в отделениях Банка

Определение контуров безопасности

Осуществление переводов денежных средств

Клиент





Банк

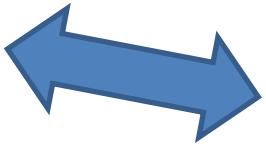
Автоматизированные банковские системы, обеспечивающие обработку платежной информации внутри Банка:

- АБС;
- Процессинговые системы

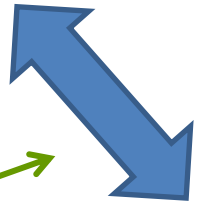
Определение контуров безопасности

Осуществление переводов денежных средств

Клиент



Банк



Автоматизированные банковские системы, обеспечивающие взаимодействие с платежными системами:

- АРМ КБР;
- SWIFT Alliance;
- Процессинговые системы

Определение 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

Устанавливается нормативными актами Банк России

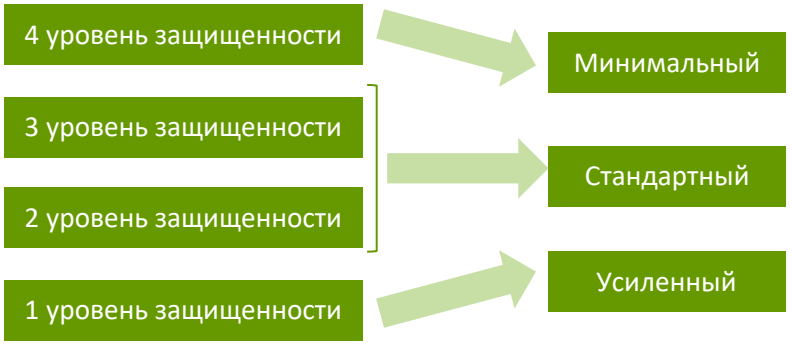
Определение уровня защиты

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

№ п/п	Контур безопасности	Нормативный документ	Уровень защиты информации	Критерий
1	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
2		п.5.3 Положения Банка России 684-П	2	Соответствующие критериям, описанным в п. 5.3 Положения
3		п.5 Положения Банка России 684-П	3	остальные

Определение уровней защиты информации

Уровни защиты для ИСПДн (рекомендуется использовать)



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

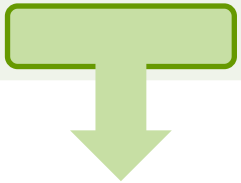
Положение Банка России 382-П

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…

Базовые требования

Процесс 1.Обеспечвение защите информации при управлении доступом

УЗП	РД
ФД	ИУ

Процесс 2. Обеспечение защиты вычислительных сетей

СМЭ	ВСА
ЗВС	ЗБС

Процесс 3. Контроль целостности и защищенности информационной инфраструктуры

Процесс 4. Защиты от вредоносного кода

Процесс 5. Предотвращение утечек информации

Процесс 6. Управление инцидентами защиты информации

МАС	РИ

Процесс 7. Защита сред виртуализации

Процесс 8. Защита информации при осуществлении удаленного логического доступа …

Базовые требования

Управление учетными записями и правами субъектов логического доступа

- ✓ организация и контроль использования субъектами логического доступа УЗ
- ✓ организация и контроль предоставления/изменения/прекращения прав доступа
- ✓ регистрация событий безопасности

Базовые требования

Пример:

УЗП.14

« Установление фактов неиспользования субъектами логического доступа предоставленных им прав на осуществление логического доступа на протяжении периода времени, превышающего 90 дней».

3	2	1
О	Т	Н

Область оценки (минимальная):

- ✓ АС
- ✓ Домен

Свидетельства:

- ✓ отчеты, акты
- ✓ правила и отчеты в SIEM

Базовые требования

Идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа

- ✓ идентификация и аутентификация субъектов логического доступа (в том числе использования многофакторной аутентификации)
- ✓ организация управления и организация защиты идентификационных и аутентификационных данных
- ✓ авторизация (разграничение доступа) при осуществлении логического доступа
- ✓ регистрация событий безопасности

Базовые требования

Примеры:

РД.6
«Аутентификация АРМ эксплуатационного персонала, используемых для осуществления логического доступа».

3	2	1
Н	Т	Т

Свидетельства:

- ✓ Настроенная MAC-аутентификация АРМ администраторов
- ✓ Использование 802.1X
- ✓ Использование систем класса NAC
- ✓ Встроенный функционал АС

Базовые требования

Процесс 1.Обеспечвение защите информации при управлении доступом

УЗП | РД

ФД | ИУ

Процесс 2. Обеспечение защиты вычислительных сетей

СМЭ | ВСА

ЗВС | ЗБС

Процесс 3. Контроль целостности и защищенности информационной инфраструктуры

Процесс 4. Защиты от вредоносного кода

Процесс 5. Предотвращение утечек информации

Процесс 6. Управление инцидентами защиты информации

МАС | РИ

Процесс 7. Защита сред виртуализации

Процесс 8. Защита информации при осуществлении удаленного логического доступа …

Защита информации при осуществлении физического доступа

- ✓ организация и контроль физического доступа в помещения
- ✓ организация и контроль физического доступа к общедоступным объектам доступа
- ✓ регистрация событий безопасности

Базовые требования

Примеры:

ФД.16
«Хранение архивов информации средств видеонаблюдения не менее
90 дней».

3	2	1
Н	Н	Т

Свидетельства:

- ✓ Выборка по помещениям и оценка глубины хранения

Базовые требования

Процесс 1.Обеспечвение защите информации при управлении доступом

УЗП | РД

ФД | ИУ

Процесс 2. Обеспечение защиты вычислительных сетей

СМЭ | ВСА

ЗВС | ЗБС

Процесс 3. Контроль целостности и защищенности информационной инфраструктуры

Процесс 4. Защиты от вредоносного кода

Процесс 5. Предотвращение утечек информации

Процесс 6. Управление инцидентами защиты информации

МАС | РИ

Процесс 7. Защита сред виртуализации

Процесс 8. Защита информации при осуществлении удаленного логического доступа …

Идентификация и учет ресурсов и объектов доступа

- ✓ учет состава ресурсов и объектов доступа
- ✓ контроль состава ресурсов и объектов доступа
- ✓ регистрация событий безопасности

Базовые требования

Примеры:

ИУ.2

«Учет используемых и (или) эксплуатируемых объектов доступа».

3	2	1
О	О	Т

Свидетельства:

- ✓ Реестры объектов доступа (с полями и реквизитами объектов доступа)
- ✓ Выгрузки из CMDB

Базовые требования

Процесс 1.Обеспечвение защите информации при управлении доступом

УЗП | РД

ФД | ИУ

Процесс 2. Обеспечение защиты вычислительных сетей

СМЭ | ВСА

ЗВС | ЗБС

Процесс 3. Контроль целостности и защищенности информационной инфраструктуры

Процесс 4. Защиты от вредоносного кода

Процесс 5. Предотвращение утечек информации

Процесс 6. Управление инцидентами защиты информации

МАС | РИ

Процесс 7. Защита сред виртуализации

Процесс 8. Защита информации при осуществлении удаленного логического доступа …

Сегментация и межсетевое экранирование вычислительных сетей

- ✓ сегментация и межсетевое экранирование внутренних вычислительных сетей
- ✓ защита внутренних вычислительных сетей при взаимодействии с сетью Интернет
- ✓ регистрация событий безопасности

Базовые требования

Примеры:

СМЭ.2

«Реализация сетевого взаимодействия и сетевой изоляции на уровне не выше третьего (сетевой), сегментов контуров безопасности и внутренних вычислительных сетей финансовой организации, не предназначенных для размещения информационной инфраструктуры, входящей в контуры безопасности».

3	2	1
Н	Т	Т

Свидетельства:

- ✓ Схема сети
- ✓ Схема адресации
- ✓ Конфигурация МЭ и/или маршрутизаторов

Базовые требования

Процесс 1.Обеспечвение защите информации при управлении доступом

УЗП

РД

ФД

ИУ

Процесс 2. Обеспечение защиты вычислительных сетей

СМЭ

ВСА

ЗВС

ЗБС

Процесс 3. Контроль целостности и защищенности информационной инфраструктуры

Процесс 4. Защиты от вредоносного кода

Процесс 5. Предотвращение утечек информации

Процесс 6. Управление инцидентами защиты информации

МАС

РИ

Процесс 7. Защита сред виртуализации

Процесс 8. Защита информации при осуществлении удаленного логического доступа …

Выявление вторжений и сетевых атак

- ✓ мониторинг и контроль содержимого сетевого трафика
- ✓ регистрация событий безопасности

Базовые требования

Примеры:

ВСА.8

«Контроль отсутствия (выявление) аномальной сетевой активности, связанной с возможным осуществлением атак типа «отказ в обслуживании», предпринимаемых в отношении ресурсов доступа, размещенных в вычислительных сетях финансовой организации, подключенных к сети Интернет».

3	2	1
Н	Т	Т

Свидетельства:

- ✓ Схема сети
- ✓ Договоры с провайдерами услуг
- ✓ Системы защиты от DDoS

Базовые требования

- Процесс 1.Обеспечвение защите информации при управлении доступом
  - УЗП
  - РД
  - ФД
  - ИУ
- Процесс 2. Обеспечение защиты вычислительных сетей
  - СМЭ
  - ВСА
  - ЗВС
  - ЗБС
- Процесс 3. Контроль целостности и защищенности информационной инфраструктуры
- Процесс 4. Защиты от вредоносного кода
- Процесс 5. Предотвращение утечек информации
- Процесс 6. Управление инцидентами защиты информации
  - МАС
  - РИ
- Процесс 7. Защита сред виртуализации
- Процесс 8. Защита информации при осуществлении удаленного логического доступа …

Защита информации, передаваемой по вычислительным сетям

Примеры:

ЗВС.2

«Реализация защиты информации от раскрытия и модификации, применение двухсторонней аутентификации при ее передаче с использованием сети Интернет, телекоммуникационных каналов и (или) линий связи, не контролируемых финансовой организацией».

3	2	1
Н	Т	Т

Свидетельства:

- ✓ Схема сети
- ✓ Описание технологии подключения территориальных подразделений, удаленный доступ
- ✓ Защита данных в системах ДБО

Базовые требования

- Процесс 1.Обеспечвение защите информации при управлении доступом
  - УЗП
  - РД
  - ФД
  - ИУ
- Процесс 2. Обеспечение защиты вычислительных сетей
  - СМЭ
  - ВСА
  - ЗВС
  - ЗБС
- Процесс 3. Контроль целостности и защищенности информационной инфраструктуры
- Процесс 4. Защиты от вредоносного кода
- Процесс 5. Предотвращение утечек информации
- Процесс 6. Управление инцидентами защиты информации
  - МАС
  - РИ
- Процесс 7. Защита сред виртуализации
- Процесс 8. Защита информации при осуществлении удаленного логического доступа …

Защита беспроводных сетей

- ✓ защиту информации от раскрытия и модификации при использовании беспроводных сетей
- ✓ защиту внутренних вычислительных сетей при использовании беспроводных сетей
- ✓ регистрация событий безопасности

Базовые требования

Контроль целостности и защищенности информационной инфраструктуры

- ✓ контроль отсутствия известных (описанных) уязвимостей защиты информации объектов информатизации
- ✓ организация и контроль размещения, хранения и обновления ПО информационной инфраструктуры
- ✓ контроль состава и целостности ПО информационной инфраструктуры
- ✓ регистрация событий безопасности

Базовые требования

Примеры:

ЦЗИ.1

«Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации, использование которых может позволить осуществить несанкционированное (неконтролируемое) информационное взаимодействие между сегментами контуров безопасности и иными внутренними сетями финансовой организации».

3	2	1
Н	Т	Т

Свидетельства:

- ✓ Схема сети и сетевой адресации
- ✓ Использование сканере безопасности
- ✓ Результаты сканирований/отчеты/периодичность

Базовые требования

Процесс 1.Обеспечвение защите информации при управлении доступом

УЗП

РД

ФД

ИУ

Процесс 2. Обеспечение защиты вычислительных сетей

СМЭ

ВСА

ЗВС

ЗБС

Процесс 3. Контроль целостности и защищенности информационной инфраструктуры

Процесс 4. Защиты от вредоносного кода

Процесс 5. Предотвращение утечек информации

Процесс 6. Управление инцидентами защиты информации

МАС

РИ

Процесс 7. Защита сред виртуализации

Процесс 8. Защита информации при осуществлении удаленного логического доступа …

Защита от вредоносного кода

- ✓ организация эшелонированной защиты от вредоносного кода на разных уровнях
- ✓ организация и контроль применения средств защиты от вредоносного кода
- ✓ регистрация событий безопасности

Базовые требования

Уровни применения средств антивирусной защиты информации на следующих уровнях:

- ✓ физических АРМ;
- ✓ виртуальной информационной инфраструктуры
- ✓ серверного оборудования
- ✓ **контроля межсетевого трафика**
- ✓ контроля почтового трафика
- ✓ входного контроля устройств и съёмных носителей информации
- ✓ общедоступных объектов доступа (ТУ ДБО)

3	2	1
Н	Т	Т

Разные вендоры:

- ✓ физических АРМ;
- ✓ серверного оборудования

3	2	1
Т	Н	Н

Разные вендоры:

- ✓ физических АРМ;
- ✓ серверного оборудования;
- ✓ контроль межсетевого трафика

3	2	1
Т	Н	Н

Базовые требования

Процесс 1.Обеспечвение защите информации при управлении доступом

УЗП | РД

ФД | ИУ

Процесс 2. Обеспечение защиты вычислительных сетей

СМЭ | ВСА

ЗВС | ЗБС

Процесс 3. Контроль целостности и защищенности информационной инфраструктуры

Процесс 4. Защиты от вредоносного кода

Процесс 5. Предотвращение утечек информации

Процесс 6. Управление инцидентами защиты информации

МАС | РИ

Процесс 7. Защита сред виртуализации

Процесс 8. Защита информации при осуществлении удаленного логического доступа …

Предотвращение утечек информации

- ✓ блокирование неразрешенных к использованию и контроль разрешенных к использованию потенциальных каналов утечки информации
- ✓ контроль (анализ) информации, передаваемой по разрешенным к использованию потенциальным каналам утечки информации
- ✓ организация защиты машинных носителей информации
- ✓ регистрация событий безопасности

Базовые требования

Процесс 1.Обеспечвение защите информации при управлении доступом

УЗП | РД

ФД | ИУ

Процесс 2. Обеспечение защиты вычислительных сетей

СМЭ | ВСА

ЗВС | ЗБС

Процесс 3. Контроль целостности и защищенности информационной инфраструктуры

Процесс 4. Защиты от вредоносного кода

Процесс 5. Предотвращение утечек информации

Процесс 6. Управление инцидентами защиты информации

МАС | РИ

Процесс 7. Защита сред виртуализации

Процесс 8. Защита информации при осуществлении удаленного логического доступа …

Контролируемые каналы:

- ✓ внешние адреса электронной почты;
- ✓ сеть Интернет;
- ✓ печать;
- ✓ съемные носители информации

3	2	1
Н	Т	Т

Способы анализа информации:

- ✓ контентный анализ;
- ✓ архивы;
- ✓ ограничения по форматам данных и размеру;
- ✓ ограничения по доступу к ресурсам сети Интернет;
- ✓ ограничения по протоколам взаимодействия
- ✓ блокирование портов;
- ✓ контроль использования съемных носителей информации

Базовые требования

Процесс 1.Обеспечвение защите информации при управлении доступом

УЗП

РД

ФД

ИУ

Процесс 2. Обеспечение защиты вычислительных сетей

СМЭ

ВСА

ЗВС

ЗБС

Процесс 3. Контроль целостности и защищенности информационной инфраструктуры

Процесс 4. Защиты от вредоносного кода

Процесс 5. Предотвращение утечек информации

Процесс 6. Управление инцидентами защиты информации

МАС

РИ

Процесс 7. Защита сред виртуализации

Процесс 8. Защита информации при осуществлении удаленного логического доступа …

Мониторинг и анализ событий защиты информации

- ✓ организация мониторинга данных регистрации о событиях защиты информации
- ✓ сбор, защиту и хранение данных регистрации о событиях защиты информации
- ✓ анализ данных регистрации о событиях защиты информации
- ✓ регистрация событий безопасности

Базовые требования

Процесс 1.Обеспечвение защите информации при управлении доступом

УЗП | РД

ФД | ИУ

Процесс 2. Обеспечение защиты вычислительных сетей

СМЭ | ВСА

ЗВС | ЗБС

Процесс 3. Контроль целостности и защищенности информационной инфраструктуры

Процесс 4. Защиты от вредоносного кода

Процесс 5. Предотвращение утечек информации

Процесс 6. Управление инцидентами защиты информации

МАС | РИ

Процесс 7. Защита сред виртуализации

Процесс 8. Защита информации при осуществлении удаленного логического доступа …

Мониторинг данных регистрации событий:

- ✓ средства и системы контроля доступа — 1
- ✓ сетевое оборудование;
- ✓ сетевые приложения и сервисы — 2
- ✓ ОС, СУБД;
- ✓ технические меры;
- ✓ АС и приложения; — 3
- ✓ Контроллер домена;

Централизованное хранение, Нормализация, фильтрация, агрегация и классификация

3	2	1
Н	Т	Т

Сроки хранения

- ✓ в течение 3 лет
- ✓ в течение 5 лет

Базовые требования

Обнаружение инцидентов защиты информации и реагирование на них

- ✓ обнаружение и регистрация инцидентов защиты информации
- ✓ организация реагирования на инциденты защиты информации
- ✓ организация хранения и защиту информации об инцидентах защиты информации
- ✓ регистрация событий безопасности

Базовые требования

- Процесс 1.Обеспечвение защите информации при управлении доступом
  - УЗП
  - РД
  - ФД
  - ИУ
- Процесс 2. Обеспечение защиты вычислительных сетей
  - СМЭ
  - ВСА
  - ЗВС
  - ЗБС
- Процесс 3. Контроль целостности и защищенности информационной инфраструктуры
- Процесс 4. Защиты от вредоносного кода
- Процесс 5. Предотвращение утечек информации
- Процесс 6. Управление инцидентами защиты информации
  - МАС
  - РИ
- Процесс 7. Защита сред виртуализации
- Процесс 8. Защита информации при осуществлении удаленного логического доступа …

✓ Регистрация информации о событиях защиты информации, потенциально связанных с инцидентами защиты информации

3	2	1
О	Т	Т

✓ Классификация инцидентов защиты информации

3	2	1
О	О	Т

✓ Установление и применение единых правил реагирования на инциденты

3	2	1
О	О	О

✓ Установление единых правил закрытия инцидентов

3	2	1
О	О	О

Базовые требования

Защита среды виртуализации (как дополнительные меры к другим процессам ГОСТ Р 57580.1-2017)

- ✓ организация идентификации, аутентификации, авторизации (разграничения доступа) при осуществлении логического доступа к виртуальным машинам и серверным компонентам виртуализации
- ✓ организацию и контроль информационного взаимодействия и изоляции виртуальных машин
- ✓ организацию защиты образов виртуальных машин
- ✓ регистрация событий безопасности

Базовые требования

Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств

- ✓ защиту информации от раскрытия и модификации при осуществлении удаленного доступа
- ✓ защиту внутренних вычислительных сетей при осуществлении удаленного доступа
- ✓ защиту информации от раскрытия и модификации при ее обработке и хранении на мобильных (переносных) устройствах
- ✓ регистрация событий безопасности

не указана в ГОСТ (?)

Базовые требования

Раздел 8 ГОСТ Р 57580.1-2017

Организационные меры защиты информации

ПЗИ.2 Состав и содержание

ПЗИ.4 Порядок применения

ПЗИ.1 Область применения процесса

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

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)

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?

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

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

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


ДиалОгНаука
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
УТВЕРЖДАЮ
Генеральный директор АО «ДиалогНаука»
_____ В.А. Сердюк
«_____» _____ 2019
Отчет
о результатах оценки соответствия требованиям ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер»
(по состоянию на 08.08.2018)
На 1 листах
Москва, 2019

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

Требования для НФО, реализующие усиленный и стандартный уровни защиты информации

Требование	Ссылка	Период.
Проведение тестирования на проникновение	п.5.4 684-П ЖЦ.20 ГОСТ 57580	ежегодно
Сертификация прикладного ПО АС	п.9 684-П	разово (а также в случаях предусмотренных выданным сертификатом)
Подписание электронных сообщений способом, позволяющим обеспечить их целостность и подтвердить их составление уполномоченным на это лицом	п.10 684-П	постоянно
Регламентация, реализация, контроль (мониторинг) технологии безопасной обработки защищаемой информации	п.11 684-П	постоянно
Регистрация событий информационной безопасности	п.12 684-П	постоянно
Внедрение процесса управления инцидентами информационной безопасности	пп.13-15 684-П	постоянно
Пересмотр применимого уровня защиты	п.5.1 684-П	ежегодно не позднее 1 рабочего дня года
Оценка выполнения требований ГОСТ Р 57580.1	п.6 684-П	ежегодно (для 1 уровня) раз в 3 года (для 2 уровня)

Спасибо за внимание!
Вопросы?

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

http://www.DialogNauka.ru