ОБЗОР НОРМАТИВНЫХ ТРЕБОВАНИЙ БАНКА РОССИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Ксения Засецкая
Старший консультант
АО «ДиалогНаука»

Москва, 09 ноября 2021

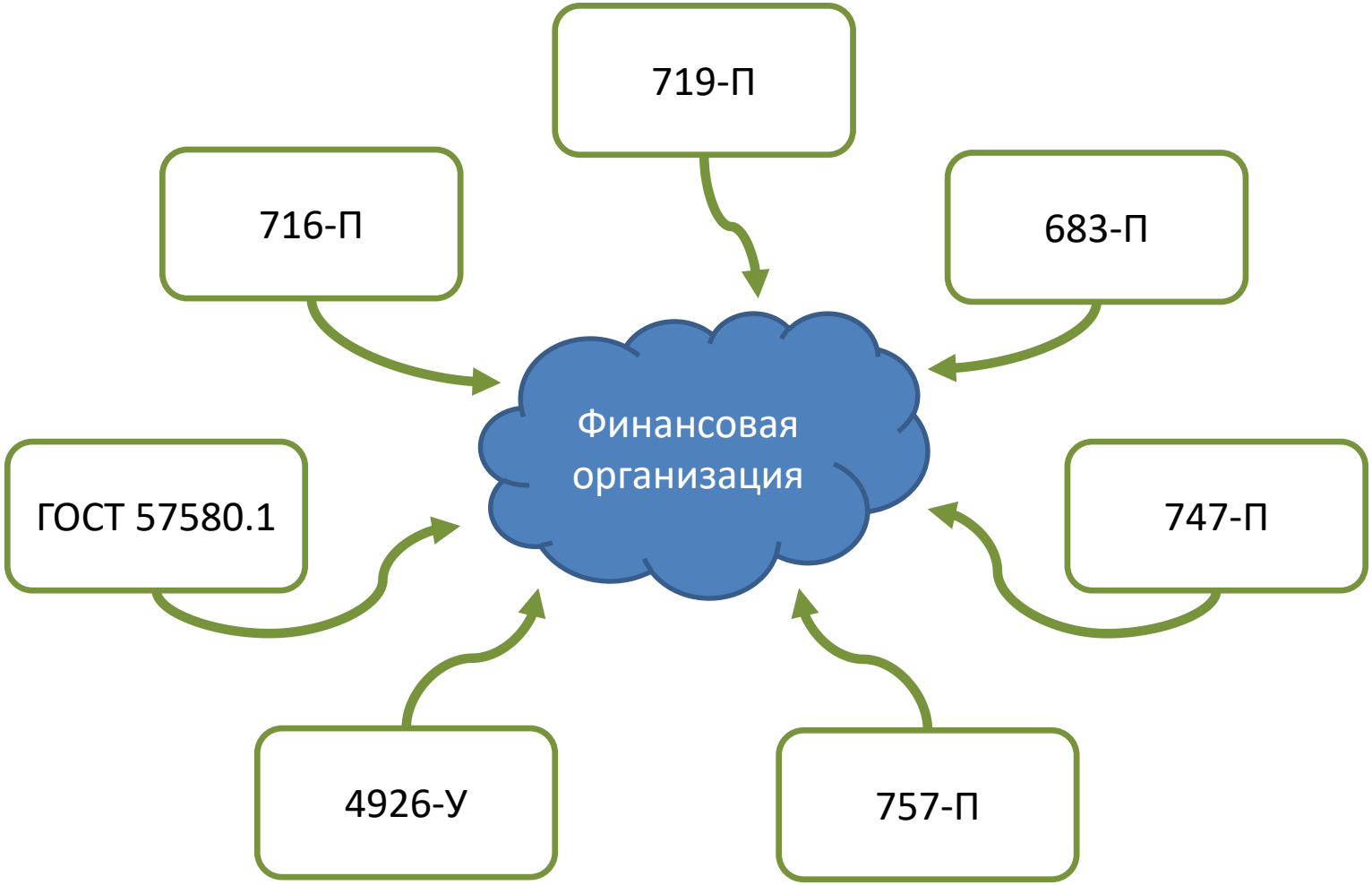
ДиалогНаука

План вебинара

В рамках вебинара будут рассмотрены следующие вопросы:

- ✓ Обзор требований и изменений в актуальных документах Банка России: 719-П, 683-П, 757-П, 747-П, ГОСТ 57580.1, 716-П, 4926-У
- ✓ Определение контуров безопасности
- ✓ Проведение оценки соответствия

Действующие требования Банка России



Положение Банка России 719-П

- ✓ оператор по переводу денежных средств (ОПДС);
- ✓ банковский платежный агент (субагент) (БПА);
- ✓ оператор услуг информационного обмена (ОУИО);
- ✓ поставщик платежного приложения (ППП);
- ✓ оператор платежной системы (ОПС);
- ✓ оператор услуг платежной инфраструктуры (ОУПИ)

Требования вступают в силу с 1 января 2022 года, кроме требований к использованию СКЗИ (вступают в силу в 2024 году и 2031 году)

Положение Банка России 719-П

- ✓ Сертификация либо оценка соответствия по ОУД 4:
  - ✓ Прикладного ПО АС и приложений, распространяемых клиентам ОПДС для совершения действий, непосредственно связанных с осуществлением переводов денежных средств;
  - ✓ ПО, эксплуатируемого на участках, используемых для приема документов, связанных с осуществлением переводов денежных средств, составленных в электронном виде, к исполнению в АС и приложениях с использованием информационно-телекоммуникационной сети «Интернет»
- ✓ Сертификация прикладного ПО АС и приложений по уровням доверия для ОПДС

Положение Банка России 719-П

- ✓ Ежегодное тестирование на проникновение и анализ уязвимостей
- ✓ Оценка соответствия раз в 2 (два) года
- ✓ Уровень соответствия не ниже 4 (четвертого) для ОПДС

Привлечение лицензиата!

Положение Банка России 683-П

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!

Положение Банка России 683-П

- 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

Положение Банка России 683-П

Системно значимые кредитные организации, кредитные организации, выполняющие функции оператора услуг платежной инфраструктуры системно значимых платежных систем, кредитные организации, значимые на рынке платежных услуг

усиленный уровень защиты информации

оценка соответствия

Не реже одного раза в 2 года

уровень соответствия не ниже третьего

с 1 января 2021 года

Положение Банка России 747-П

Часть требований – с 01.01.2022
Часть – с 01.07.2022

ПС БР

Участники ССНП

Участники СБП

ОПКЦ

ОУИО СБП

С 01.01.2023 – уровень соответствия не ниже 4!

Положение Банка России 747-П

Участники ССНП
Участники СБП

→ **стандартный уровень защиты информации**

оценка соответствия

→ Не реже одного раза в 2 года

уровень соответствия не ниже четвертого

→ **с 1 января 2023 года**

Положение Банка России 757-П

Усиленный уровень защиты

- ✓ Центральные контрагенты
- ✓ Центральный депозитарий
- ✓ Регистраторы финансовых транзакций (с 01.01.2022)

Стандартный уровень

- ✓ специализированные депозитарии инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов;
- ✓ клиринговые организации;
- ✓ организаторы торговли;
- ✓ страховые организации (…);
- ✓ НПФ, осуществляющие деятельность по обязательному пенсионному страхованию;
- ✓ НПФ
- ✓ брокеры, дилеры (…) и иные организации

Положение Банка России 757-П

Минимальный уровень

- ✓ специализированные депозитарии инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов (часть);
- ✓ часть брокеров и дилеров;
- ✓ УК инвестиционных фондов, паевых ИФ и НПФ;
- ✓ форекс-дилеры;
- ✓ страховые организации и страховые брокеры и иные организации

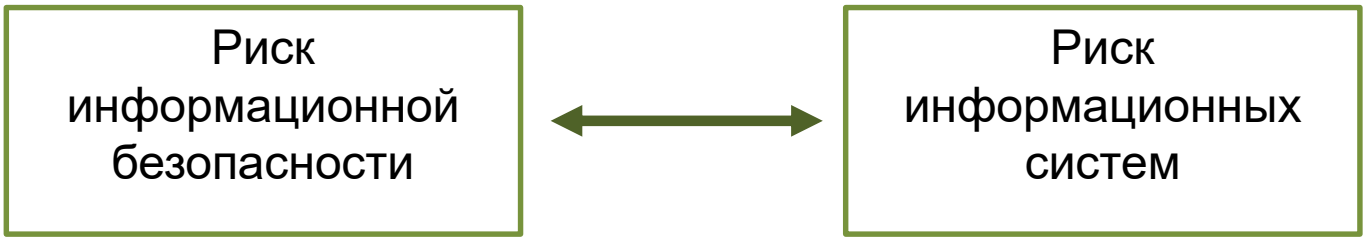
Усиленный и стандартный уровни

- ✓ ежегодное тестирование на проникновение;
- ✓ оценка соответствия с привлечением лицензиата;
- ✓ оценка соответствия ежегодно либо раз в три года (для разных уровней);
- ✓ Сертификация прикладного ПО АС и приложений, распространяемых клиентам для совершения действий в целях осуществления финансовых операций, а также ПО, обрабатывающего защищаемую информацию при приеме электронных сообщений

С 01.01.2022 – уровень соответствия не ниже 3 для усиленного и стандартного уровней защиты!

Положение Банка России 716-П

- ✓ Подход к управлению рисками информационной безопасности
- ✓ Погружение в операционные риски
- ✓ Требования к внутренним документам
- ✓ Вовлеченность в процесс управления рисками ИБ



Указание Банка России 4926-У

Информирование Банка России об инцидентах

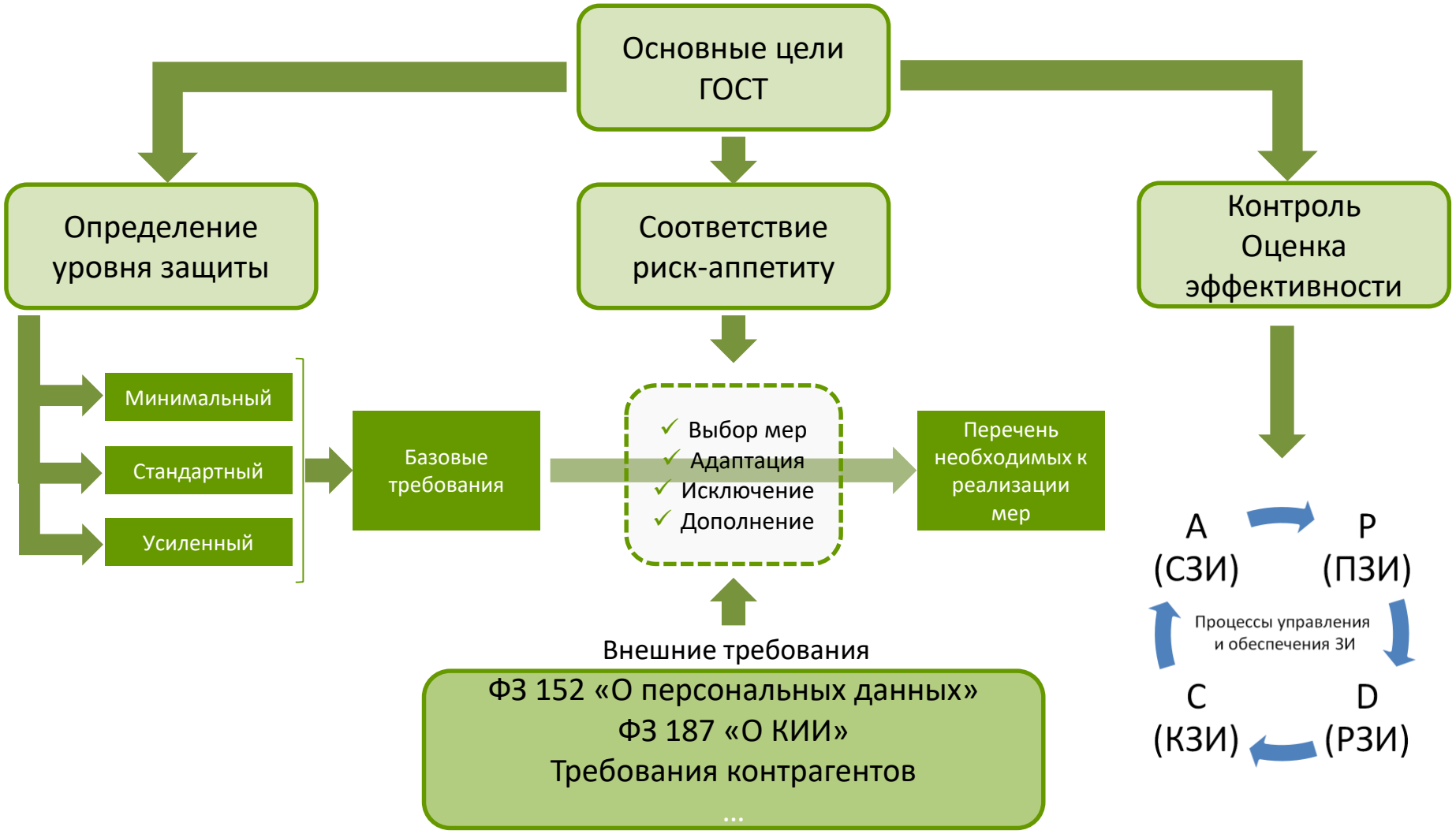
Выявление несанкционированных операций

Осуществление сбора технических данных

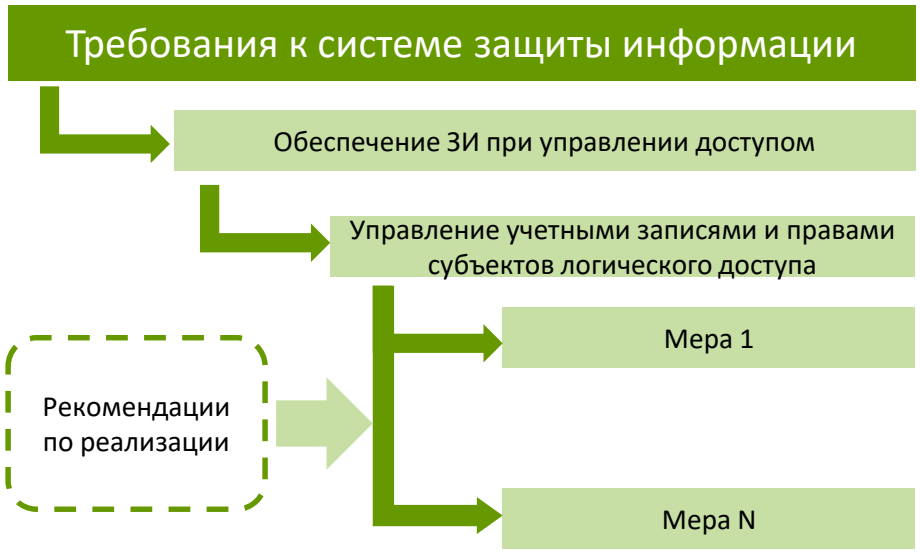
Выявление, анализ и устранение причин

Совершенствование системы

ГОСТ Р 57580.1-2017



Базовые требования



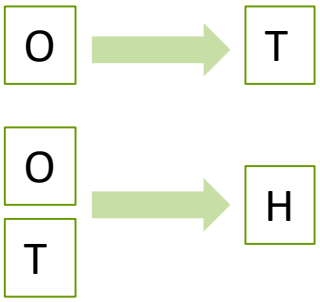
Направление — 3 направления

Процесс — 8 процессов

Подпроцесс

Меры системы защиты информации — 343 меры

Примечание:



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

Сроки

01.01.2020
Необходимость сертификации прикладного ПО АС

25.02.2021
Вступило в силу 747-П

01.01.2021
1. Необходимость выполнения требований ГОСТ Р 57580.1-2017
2. Уровень не ниже 3 для КО
3. Проведение тестирований на проникновение
4. Проведение оценки соответствия

01.07.2021
Дополнительные требования 747-П

02.07.2021
Вступило в силу 757-П

01.01.2022
Необходимость обеспечения не ниже 3 уровня соответствия для НФО
ГОСТ Р 57580.1-2017
Вступает в силу 719-П
Дополнительные требования 747-П
Требования 757-П
Готовность к 716-П

01.07.2021
Дополнительные требования 747-П
Дополнительные требования 757-П

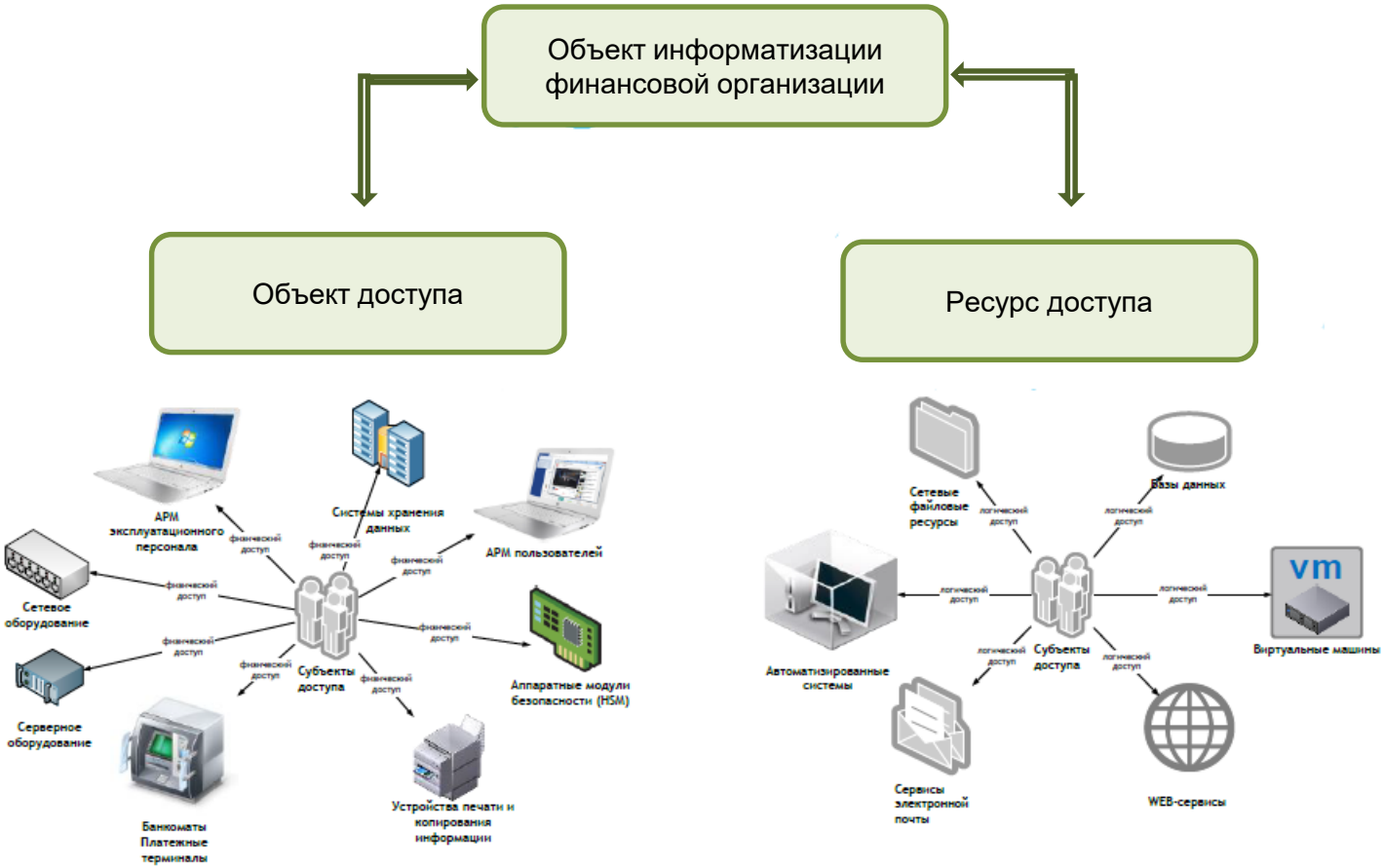
01.01.2023
Необходимость обеспечения не ниже 4 уровня соответствия ГОСТ Р 57580.1-2017 для КО
Дополнительные требования 747-П

01.07.2023
Необходимость обеспечения не ниже 4 уровня соответствия ГОСТ Р 57580.1-2017 для НФО
Дополнительные требования 757-П

01.01.2024
Дополнительные требования 757-П
Дополнительные требования 719-П

Определение контуров безопасности

- ✓ Как правильно определять контуры безопасности?



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 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 к порядку осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств

Положения Банка России:
- ✓ 747-П
- ✓ 683-П
- ✓ 757-П

Методические рекомендации
- ✓ 4-МР

Определение контуров безопасности

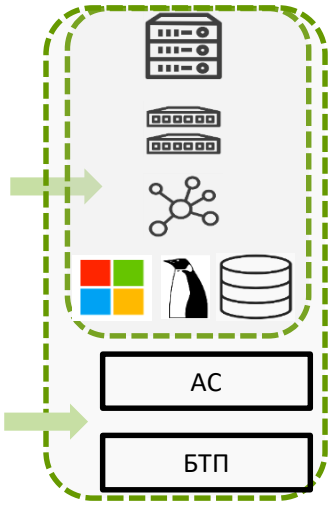
Цитата:

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

Совокупность объектов информатизации

Уровни информационной инфраструктуры:

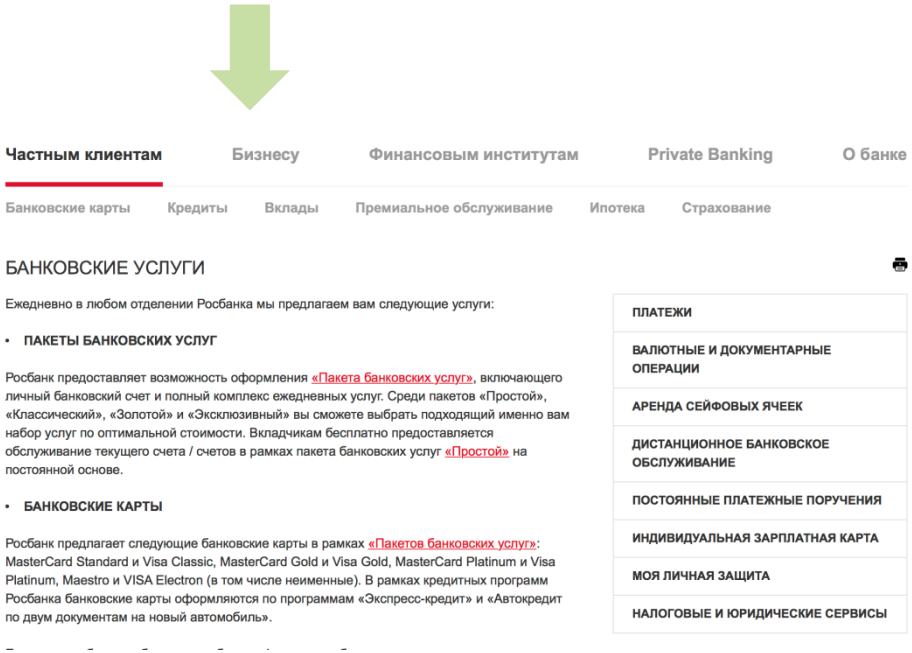
- ✓ Системный уровень
- ✓ Уровень АС и приложений



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».

Единая степень критичности

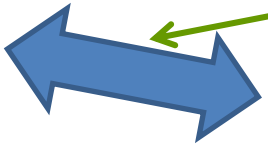
Единая политика защиты информации

Контур безопасности

Определение контуров безопасности

Осуществление переводов денежных средств

Клиент



Банк

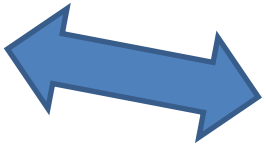
Автоматизированные банковские системы, обеспечивающие взаимодействие с клиентами Банка:

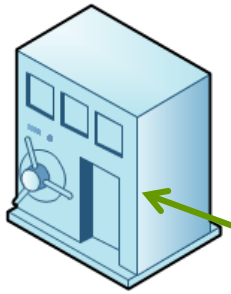
- удаленное взаимодействие (Системы ДБО)
- взаимодействие в отделениях Банка

Определение контуров безопасности

Осуществление переводов денежных средств

Клиент





Банк

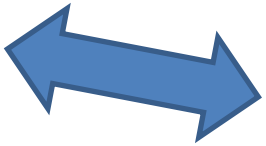
Автоматизированные банковские системы, обеспечивающие обработку платежной информации внутри Банка:

- АБС;
- Процессинговые системы

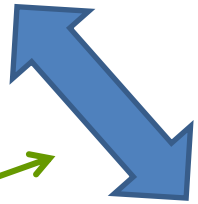
Определение контуров безопасности

Осуществление переводов денежных средств

Клиент



Банк



Банк России

SWIFT

Автоматизированные банковские системы, обеспечивающие взаимодействие с платежными системами:

- АРМ КБР;
- SWIFT Alliance;
- Процессинговые системы

VISA

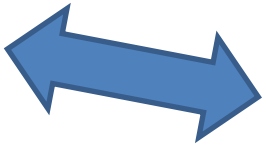
mastercard

НСПК
НАЦИОНАЛЬНАЯ СИСТЕМА ПЛАТЕЖНЫХ КАРТ

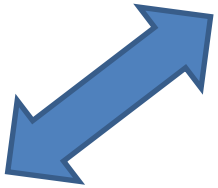
Определение контуров безопасности

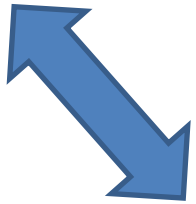
Осуществление переводов денежных средств

Клиент



Банк





Банк

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?

Методика. Формулы

Требования к системе защиты информации

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

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

Если в область оценки соответствия входят несколько контуров безопасности разного уровня

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

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

Интерпретация результатов оценки

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

Рекомендуемый ЦБ

Итоговая оценка соответствия ЗИ ***R***

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

Требования к отчетным документам

Отчет о результатах оценки соответствия требованиям ГОСТ

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

Возможные санкции

- ✓ Федеральный закон от 27.06.2011 N 161-ФЗ «О национальной платежной системе»

Статья 34. Действия и меры принуждения, применяемые Банком России в случае нарушения поднадзорной организацией требований настоящего Федерального закона или принятых в соответствии с ним нормативных актов Банка России
Последствия – **приостановление деятельности по переводу денежных средств**

- ✓ КоАП РФ. ч. 6 Ст. 13.12. Нарушение правил защиты информации

Нарушение требований о защите информации (за исключением информации, составляющей государственную тайну), установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, за исключением случаев, предусмотренных частями 1, 2 и 5 настоящей статьи, -
влечет наложение **административного штрафа** на граждан в размере от пятисот до одной тысячи рублей; на должностных лиц - **от одной тысячи до двух тысяч рублей**; на юридических лиц - **от десяти тысяч до пятнадцати тысяч рублей**

- ✓ КоАП РФ. ч. 9 Ст. 19.5

Невыполнение в установленный срок законного предписания Банка России - влечет наложение **административного штрафа** на должностных лиц в размере **от двадцати тысяч до тридцати тысяч рублей**; на юридических лиц - **от пятисот тысяч до семисот тысяч рублей**

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