ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Как жить с новой отчётностью по защите информации для Банков?



Алексей Глазков

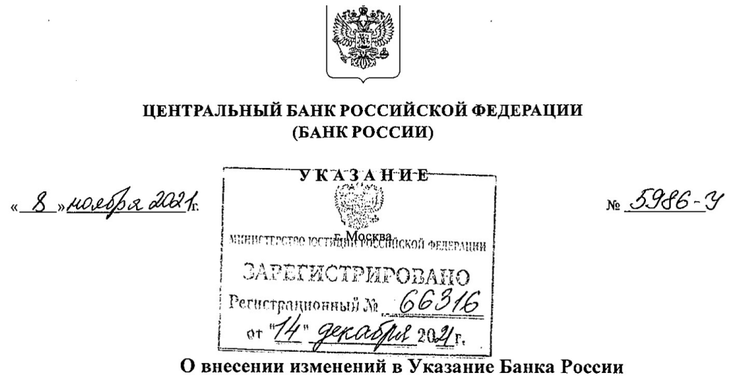
Руководитель обособленного подразделения
«Перспективный мониторинг» в г. Пенза

Указание Банка России
№ 5986-У

Указание Банка России от 8 ноября 2021 г. №5986-У
«О внесении изменений в Указание БР №4927-У»
было зарегистрировано 14 декабря 2021 года.

Настоящее Указание вступает в силу с 31 марта 2022 года.

**Всё, что относится к форме 0409071,
вступает в силу с 1 октября 2022 года.**



ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

УКАЗАНИЕ

«8» ноября 2021 г. № 5986-У

г. Москва

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 66316
от "14" декабря 2021 г.

О внесении изменений в Указание Банка России от 8 октября 2018 года № 4927-У «О перечне, формах и порядке составления и представления форм отчетности кредитных организаций в Центральный банк Российской Федерации»

На основании части первой статьи 57 Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» (Собрание законодательства Российской Федерации, 2002, № 28, ст. 2790), части первой статьи 43 Федерального закона «О банках и банковской деятельности» (в редакции Федерального закона от 3 февраля 1996 года № 17-ФЗ) (Ведомости Съезда народных депутатов РСФСР и Верховного Совета РСФСР, 1990, № 27, ст. 357; Собрание законодательства Российской Федерации, 1996, № 6, ст. 492; 2013, № 27, ст. 3438) и в соответствии с решением Совета директоров Банка России (протокол заседания Совета директоров Банка России от 11 октября 2021 года № ПСД-24):

1. Внести в Указание Банка России от 8 октября 2018 года № 4927-У «О перечне, формах и порядке составления и представления форм отчетности кредитных организаций в Центральный банк Российской Федерации», зарегистрированное Министерством юстиции Российской Федерации 13 декабря 2018 года № 52992, 13 декабря 2019 года № 56796,

По каким требованиям оценивать?

Самооценка

- Положение № 683-П
- Положение № 747-П
- Положение № 757-П
- Положение № 719-П

Внешняя оценка соответствия

- ГОСТ Р 57580.1

Форма 0409071

Раздел 1

- Сведения об оценке выполнения требований по направлению «Технологические требования»;

Раздел 2

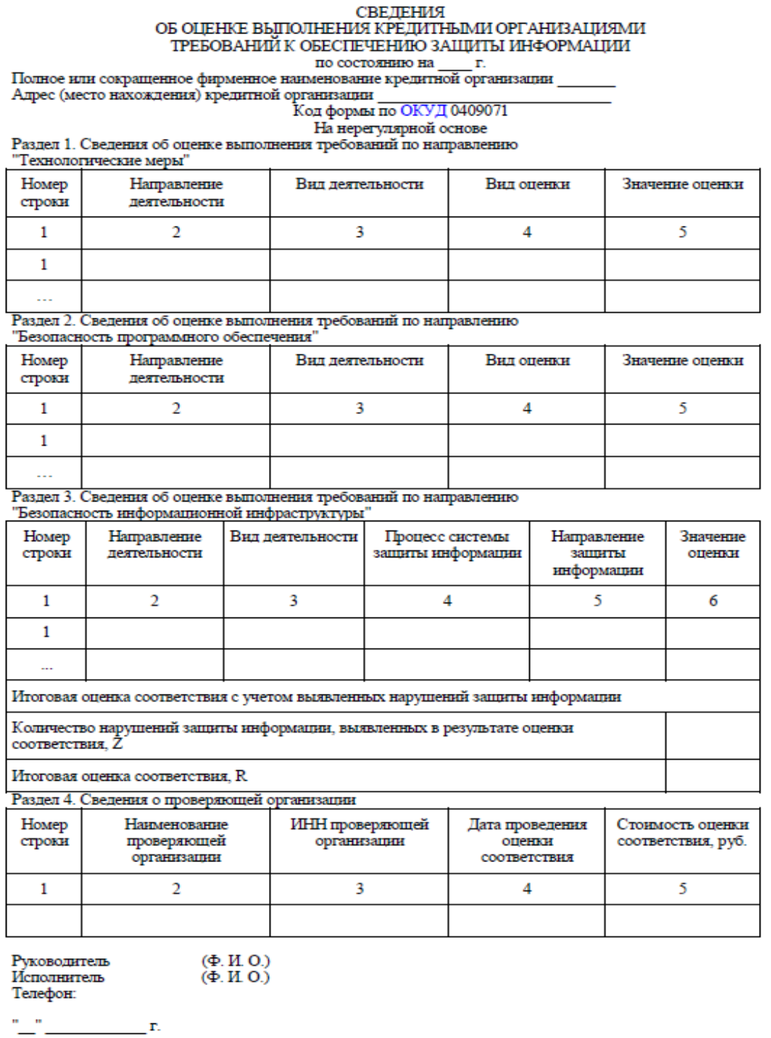
- Сведения об оценке выполнения требований по направлению «Безопасность программного обеспечения»;

Раздел 3

- Сведения об оценке выполнения требований по направлению «Безопасность информационной инфраструктуры» *(оценка соответствия требованиям ГОСТ Р 57580.1);*

Раздел 4

- Сведения о проверяющей организации



СВЕДЕНИЯ
ОБ ОЦЕНКЕ ВЫПОЛНЕНИЯ КРЕДИТНЫМИ ОРГАНИЗАЦИЯМИ
ТРЕБОВАНИЙ К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ
по состоянию на ____ г.

Полное или сокращенное фирменное наименование кредитной организации _____
Адрес (место нахождения) кредитной организации _____
Код формы по ОКУД 0409071
На нерегулярной основе

Раздел 1. Сведения об оценке выполнения требований по направлению "Технологические меры"

Номер строки	Направление деятельности	Вид деятельности	Вид оценки	Значение оценки
1	2	3	4	5
1				
...				

Раздел 2. Сведения об оценке выполнения требований по направлению "Безопасность программного обеспечения"

Номер строки	Направление деятельности	Вид деятельности	Вид оценки	Значение оценки
1	2	3	4	5
1				
...				

Раздел 3. Сведения об оценке выполнения требований по направлению "Безопасность информационной инфраструктуры"

Номер строки	Направление деятельности	Вид деятельности	Процесс системы защиты информации	Направление защиты информации	Значение оценки
1	2	3	4	5	6
1					
...					
Итоговая оценка соответствия с учетом выявленных нарушений защиты информации					
Количество нарушений защиты информации, выявленных в результате оценки соответствия, Z					
Итоговая оценка соответствия, R					

Раздел 4. Сведения о проверяющей организации

Номер строки	Наименование проверяющей организации	ИНН проверяющей организации	Дата проведения оценки соответствия	Стоимость оценки соответствия, руб.
1	2	3	4	5

Руководитель (Ф. И. О.)
Исполнитель (Ф. И. О.)
Телефон:

"__" _____ г.

Проблемы заполнения формы 0409071

Было

Общие требования к обеспечению защиты информации
1) Требование, указанное в подпункте 5.1 пункта 5 Положения Банка России N 683-П
Требования к обеспечению защиты информации, применяемые на технологическом участке формирования (подготовки), передачи и приёма электронных сообщений
4) Требование, указанное в абзаце третьем подпункта 5.2.1 пункта 5 Положения Банка России N 683-П

Стало

№ 683-П	Оценка соответствия выполнения требований Положения Банка России № 683-П
№ 719-П	Оценка соответствия выполнения требований Положения Банка России № 719-П
№ 747-П	Оценка соответствия выполнения требований Положения Банка России № 747-П
№ 757-П	Оценка соответствия выполнения требований Положения Банка России № 757-П

Проблемы заполнения формы 0409071

Было

$$E_{\text{ТМП}} = \frac{\sum_{i=1}^{N} E_{\text{По}_i} + \sum_{i=1}^{N} E_{\text{Пп}_i}}{2N},$$

Оценка выполнения требований планирования применения мер защиты информации ($E_{тмп}$)

1) Определена ли область применения меры защиты информации?
2) Определён ли порядок применения меры защиты информации?

Оценка ответов производится путём присвоения им значений:

1 — «да» (определено); **0** — «нет» (не определено)

Стало

($E_{тмп}$) — планирование

($E_{тмр}$) — реализация

($E_{тмк}$) — контроль

($E_{тмс}$) — совершенствование

($E_{тм}$) — технологические меры

Осталась таблица с кодами оценок и требование указать значение оценок

Раздел 1 формы 0409071

Направление деятельности	Вид деятельности	Вид оценки	Значение оценки
№ 683-П	**Банк**	($E_{ТМП}$)	**1**
		($E_{ТМР}$)	**0,87**
		($E_{ТМК}$)	**0,71**
		($E_{ТМС}$)	**0,5**
		($E_{ТМ}$)	**0,81**
№ 719-П	**ОПДС,** ОУПИ РЦ, ОУПИ ОЦ, ОУПИ ПКЦ		
№ 747-П	Участник ПС БР		
№ 757-П	Брокер, Дилер, Депозитарий, ДУ, СД, ЦК, ЦД, РФТ, Репозитарий, ОИП, ОИС, ЦФА		

Раздел 2 формы 0409071

Направление деятельности	Вид деятельности	Вид оценки	Значение оценки
№ 683-П	**Банк**	$E_{поп}$	
		$E_{пор}$	
		$E_{пок}$	
		$E_{пос}$	
		$E_{по}$	
		ППО ОС	сертификация ФСТЭК России / оценка соответствия ОУД
№ 719-П	**ОПДС,** ОУПИ		
№ 757-П	Брокер, Дилер, Депозитарий, ДУ, СД, ЦК, ЦД, РФТ, Репозитарий, ОИП, ОИС, ЦФА		

Раздел 3 формы 0409071

Направление и вид деятельности	Процесс системы ЗИ	Направление ЗИ	Значение оценки
№ 683-П (Банк)	1-8	$E_{ПЗИi}$	**0,73**
		E_{Pi}	**0,6**
№ 719-П (ОПДС, ООУПИ)		$E_{Пi}$	**0,5**
		E_{Ki}	**0,18**
№ 747-П (Участник ПС БР)		E_{Ci}	**0,38**
		$E_{АС}$	$E_{АС}$
№ 757-П (Брокер, Дилер, Депозитарий, ДУ, СД, ЦК, ЦД, РФТ, Репозитарий, ОИП, ОИС, ЦФА		Уровень соответствия	Второй
		E_i	**0, 59**
	Применение организационных и технических мер ЗИ на этапах ЖЦ АС	$E_{АС}$	**0, 75**
		Уровень соответствия	Третий
Итоговая оценка соответствия с учетом выявленных нарушений защиты информации			
Количество нарушений защиты информации, выявленных в результате оценки соответствия, Z			0
Итоговая оценка соответствия, R			0,72 (Трети

Не на своём месте???

Вероятно, оценка по ЖЦ АС должна быть здесь

Как часто отчитываться?

Кредитным организациям, при совмещении деятельности с деятельностью некредитной финансовой организации, реализующей усиленный уровень защиты информации (*центральные контрагенты; центральный депозитарий; регистраторы финансовых транзакций).*

1

раз в год не позднее

30

рабочих дней

Как часто отчитываться?

Кредитным организациям:

- осуществляющим банковскую деятельность
- являющимися операторами по переводу денежных средств (ОПДС) и (или) операторами услуг платежной инфраструктуры (ОУПИ)
- осуществляющими деятельность расчётного центра (Участники ССНП, участники СБП, ОПКЦ и ОУИО СБП)
- осуществляющими деятельность участника платёжной системы Банка России

1

раз в два года не позднее

30

рабочих дней

Как часто отчитываться?

Кредитным организациям, при совмещении деятельности с деятельностью некредитной финансовой организации, реализующей стандартный уровень защиты информации.

К таким НФО относятся: специализированные депозитарии инвестиционных фондов, паевые инвестиционные фонды и негосударственные пенсионные фонды; клиринговые организации; организаторы торговли; страховые организации; негосударственные пенсионные фонды; репозитарии, не являющиеся регистраторами финансовых транзакций; брокеры, дилеры, управляющие, депозитарии и регистраторы; операторы инвестиционной платформы; операторы финансовой платформы и др.

1

раз в три года не позднее

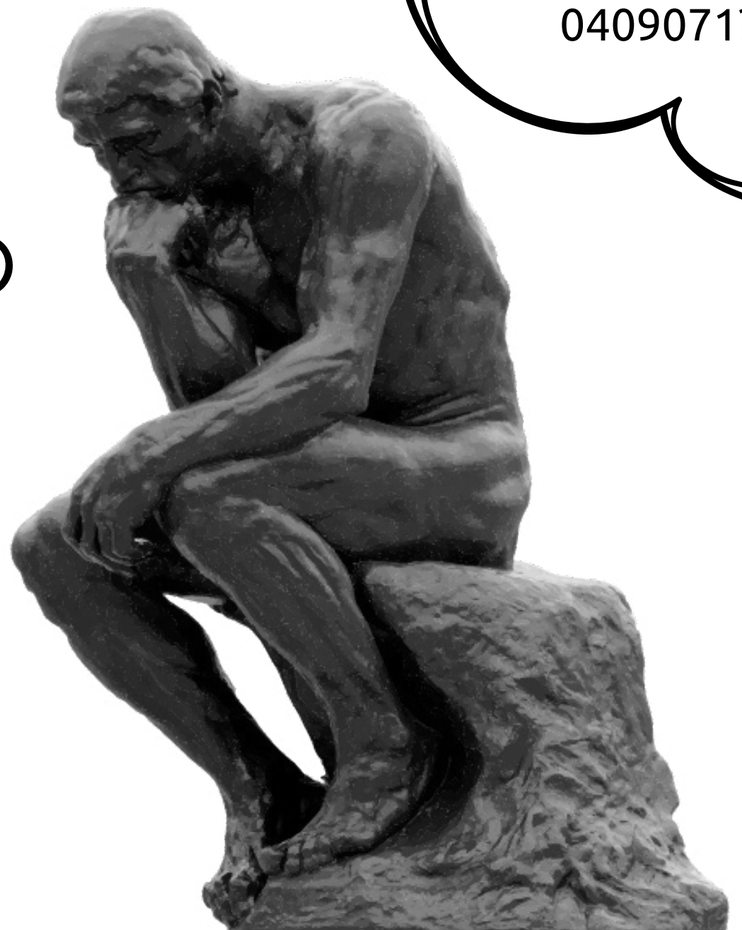
30

рабочих дней

Как жить дальше?

Ждем очередных нормативных документов от Центрального банка Российской Федерации…

Когда появится методика заполнения формы отчётности 0409071???



Оценка соответствия требованиям ГОСТ Р 57580.1, проведённая до 01.10.2022 г. засчитывается???

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Обеспечение соответствия требованиям ГОСТ Р 57580.1 при аутсорсинге ИТ и ИБ



Алексей Глазков

Руководитель обособленного подразделения
«Перспективный мониторинг» в г. Пенза

Почему идём
на аутсорсинг ИТ и ИБ?



Высокая стоимость квалифицированных специалистов



Получение высококачественной услуги



Избавление от непрофильных видов деятельности

О чём надо помнить!

Банковская тайна



Подводные камни

1. 
Ответственность перед **клиентами** полностью лежит на кредитной организации

2. 
Договор в виде присоединения к Соглашению

3. 
Зависимость от поставщика

4. 
От ИТ аутсорсинга неотрывны задачи ИБ

5. 
Контроль ИБ затруднён

6. 
Неопределённость в выполнении регуляторных требований

7. 
Непрозрачность внутренней практики поставщика услуг по обеспечению ИБ

Как минимизировать риски?



СТО БР ИББС-1.4-2018

СТАНДАРТ БАНКА РОССИИ

СТО БР ИББС-1.4-2018

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

УПРАВЛЕНИЕ РИСКОМ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ АУТСОРСИНГЕ

Дата введения: 2018-07-01

Издание официальное

Оцените риски
применения аутсорсинга

1. Несоблюдение требований законодательства
2. Затруднение контроля ИБ поставщиком услуг
3. Возможность деградации или прерывания услуг в результате реализации угроз ИБ
4. Возникновение зависимости от поставщика услуг

Оцените
поставщика услуг

- Деловая репутация
- Финансовые показатели
- Наличие необходимых лицензий
- Наличие профессиональных сертификатов
- Подходы по обеспечению непрерывности оказания услуг (787-П)
- Наличие обученного персонала

SLA

1) **Состав предоставляемых сервисов**

2) **Согласованный уровень качества сервиса**

- описание расчёта ключевых параметров качества сервиса и периодичность предоставления отчётов о параметрах качества
- методы и средства контроля ключевых параметров качества
- описание методов контроля исполнения SLA
- установление обязанности и описание процедуры предоставления услуг информации
- описание процедур восстановления работы в случаях прерывания предоставляемых сервисов



Контроль
поставщика услуг

Определите мероприятия и правила контроля поставщика услуг



Например:

- Установите обязанность прохождения оценки соответствия (в части ЗИ - ГОСТ Р 57580.1, ГОСТ Р ИСО/МЭК 27001 и др.)
- Определите пул аудиторов которым вы доверяете
- Установите обязанность предоставления запрашиваемой проверяющими организациями информации

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Спасибо
за внимание!

Алексей Глазков

Руководитель обособленного
подразделения компании
«Перспективный мониторинг»
в г. Пенза

Aleksey.Glazkov@amonitoring.ru