RTM GROUP

Порядок составления и представления отчетности по форме 0409071 “Сведения об оценке выполнения кредитными организациями требований к обеспечению защиты информации”

RTM GROUP

Объединяем IT,
право и безопасность

Далее

Спикер

Дмитрий Кобец

- **Заместитель директора** технического Департамента
- **Эксперт** в сфере информационной безопасности
- **Профессиональный опыт** в сфере информационных технологий и информационной безопасности с 2009 года

О компании RTM Group

RTM Group — ведущая консалтинговая компания в области информационной безопасности, судебной экспертизы и ИТ-права.

Информационная безопасность:

Аудиты, пентест, КИИ, защита ПДн, оценка защищённости и др.

Компьютерно-технические экспертизы:

44-ФЗ, расследования инцидентов, ИТ-контракты и др.

ИТ-право:

Судебное и досудебное урегулирование, сопровождение и др.

СОДЕРЖАНИЕ

01. Основные изменения

Указание Банка России от 18.02.2022 N 6071-У

"О внесении изменений в Положение Банка России от 17 апреля 2019 года N 683-П "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".

(Зарегистрировано в Минюсте России 20.06.2022 N 68919)

01. Основные изменения: ОУД 4 и сертификация

П. 4.1.

Было	Стало
Сертификация ПО на отсутствие НДВ или анализ уязвимостей по ОУД4	Сертификация ПО по 76 приказу ФСТЭК или оценка соответствия по ОУД4
К анализу по ОУД4 привлекать лицензиатов ФСТЭК	При выборе сертификации – 4 уровень для значимых банков и 5 для иных
	Оценка соответствия самостоятельно или привлечение лицензиатов ФСТЭК

01. Основные изменения: электронные сообщения

П. 5.1.

Было	Стало
Подписание способом, позволяющим обеспечить целостность	Обеспечить целостность
	Использование УКЭП, УНЭП, СКЗИ с имитозащитой*
	Случаи неприменения УКЭП, УНЭП, СКЗИ с имитозащитой*

*** Имитозащита** – защита целостности сообщения. Реализуется с помощью добавления к сообщению дополнительного кода, имитовставки, MAC, зависящей от содержания сообщения и секретного элемента, известного только отправителю и получателю (ключа).

01. Основные изменения: технология обработки защищаемой информации

П. 5.2.1

Было	Стало
Подтверждение совершенной операции.	Идентификация устройств клиентов
	Проверка абонентского номера
	Подтверждение совершаемой операции
	Подтверждение адреса электронной почты.

01. Основные изменения: ограничения по параметрам операций

П. 7

Было	Стало
Вариант без изменений	**Добавлен П. 7.1** «Ограничения по параметрам операции»

Похожее требование встречалось в Положении Банка России № 382-П.

01. Основные изменения: требования к управлению инцидентами

П. 8

Было	Стало
Регистрация инцидентов.	Значения инцидентов в п.7.3 Положения 716-П
	Фиксация инцидентов в базе событий
	Информирование регулятора о принятых мерах по реагированию
	Информирование о сайтах в сети «Интернет»
	Предоставлять сведения регулятору через АС ЦБ РФ

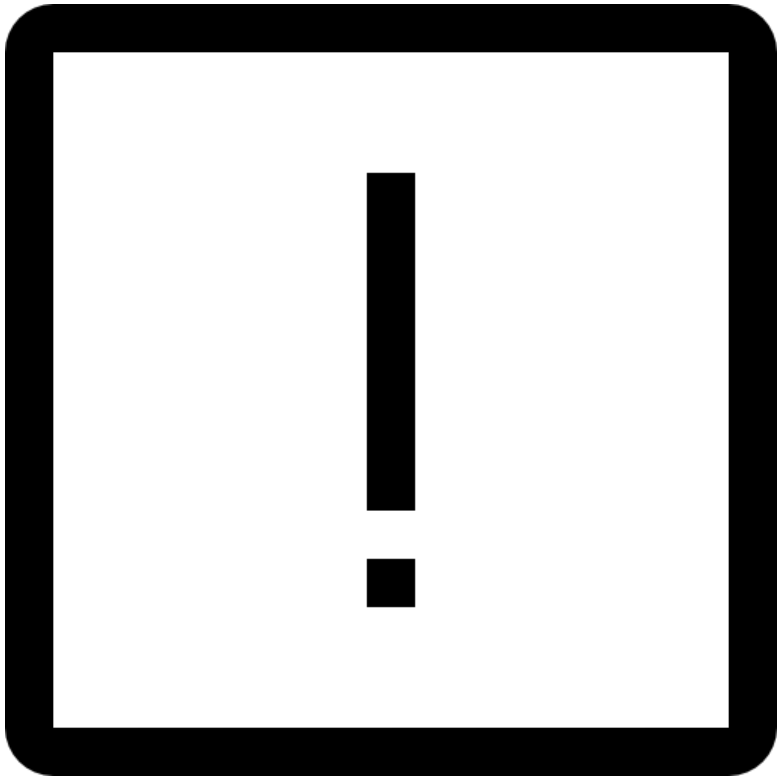
01. Основные изменения: КИИ

П. 10

Было	Стало
Вариант без изменений	При обеспечении безопасности ПО, СВТ, Положение применяется наряду с требованиями 187-ФЗ

01. Основные изменения: последствия неисполнения

1. **Штрафные санкции со стороны регулятора**
2. **Рост риска несанкционированных списаний**
3. **Рост риска возникновения уязвимостей**



02. Порядок составления и представления отчетности по форме 0409071. Нормативно-правовая база

1. **Указание № 5986-У** от 08 ноября 2021 г. «О внесении изменений в Указание Банка России » от 08.10.2018.

2. **Указание №4927-У** «О перечне, формах и порядке составления и предоставления форм отчетности кредитных организаций в Центральный банк Российской Федерации» (Вступает в силу с 31.03.2022 г).

02. Порядок составления и представления отчетности по форме 0409071. Кто обязан сдавать отчеты по видам деятельности?

02. Порядок составления и представления отчетности по форме 0409071. Кто обязан сдавать отчеты по видам деятельности?

Направление деятельности	Вид деятельности	Вид оценки	Значение оценки
2	3	4	5
№ 683-П	ОПДС	Етмп	0,85
		Етмр	0,86
		Етмк	0,79
		Етмс	0,84
		Етм	0,84

Раздел включает в себя **оценку технологических мер** положения в соответствии с методикой, изложенной в Приложении 1 к Положению Банка России от 3 декабря 2020 года N 742-П.

Планирование

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

- *i – порядковый номер меры*
- *N – общее количество мер*
- $E_{\text{По}_i}$ *– значение оценки меры защиты, по вопросу определения области защиты (0/1)*
- $E_{\text{Пп}_i}$ *– значение оценки меры защиты, по вопросу порядка применения мер защиты (0/1)*

Реализация

$$E_{\text{TMP}} = \frac{\sum_{i=1}^{N} E_{\text{Рм}_i}}{N},$$

- **1 – "да"** ("постоянно", "всегда", "в полном объеме");
- **0.75** – **"в основном да"** ("почти постоянно", "почти всегда", "почти в полном объеме");
- **0.5 – "частично"** ("отчасти да", "не всегда", "в некоторых случаях");
- **0.25 – "в основном нет"** ("непостоянно", "почти никогда");
- **0 – "нет"** ("никогда", "ни в каких случаях").

i – порядковый номер меры

N – общее количество мер

$E_{\text{Рм}_i}$ *– значение оценки меры защиты, в рамках процесса реализации (0/0,25/0,5/0,75/1)*

Контроль

$$E_{\text{ТМК}} = \frac{\sum_{i=1}^{N} E_{\text{Ко}_i} + \sum_{i=1}^{N} E_{\text{Кп}_i} + \sum_{i=1}^{N} E_{\text{Кз}_i}}{3N},$$

- *i – порядковый номер меры*
- *N – общее количество мер*
- $E_{\text{Ко}_i}$ *– значение оценки меры защиты, по вопросу контроля* ***области применения*** *мер защиты (0/1)*
- $E_{\text{Кп}_i}$ *– значение оценки меры защиты, по вопросу контроля* ***должного применения*** *мер защиты (0/1)*
- $E_{\text{Кз}_i}$ *– значение оценки меры защиты, по вопросу контроля* ***знаний работников*** *в части применения мер защиты (0/1)*

Совершенствование

$$E_{\text{ТМС}} = \frac{\sum_{i=1}^{N} E_{\text{Си}_i} + \sum_{i=1}^{N} E_{\text{Сн}_i}}{2N},$$

- *i – порядковый номер меры*
- *N – общее количество мер*
- $E_{\text{Си}_i}$ *– значение оценки меры защиты в рамках процесса совершенствования, по вопросу анализа необходимости совершенствования мер ЗИ, в случае обнаружения* ***инцидентов*** *(0/1)*
- $E_{\text{Сн}_i}$ *– значение оценки меры защиты в рамках процесса совершенствования, по вопросу анализа необходимости совершенствования мер ЗИ, в случае обнаружения* ***недостатков*** *(0/1)*

Расчёт направлений технологических мер: итоговая оценка

$$E_{\text{ТМ}} = 0{,}2E_{\text{ТМП}} + 0{,}4E_{\text{ТМР}} + 0{,}25E_{\text{ТМК}} + 0{,}15E_{\text{ТМС}},$$

Автоматизация

N п/п	Технологические меры защиты информации	Епо	Епп	Ерм	Еко	Екп	Екз	Еси	Есн
1	Технология обработки защищаемой информации обеспечивает подписание электронных сообщений (указаний) способом, позволяющим обеспечить их целостность и подтвердить их составление уполномоченным на это лицом	1	1	1	1	1	1	1	1
2	Технология обработки защищаемой информации, применяемая на всех технологических участках, обеспечивает целостность и неизменность защищаемой информации	1	1	1	1	1	1	1	1
3	Технология обработки защищаемой информации обеспечивает применение механизмов и (или) протоколов формирования и обмена электронными сообщениями, обеспечивающих защиту электронных сообщений от искажения, фальсификации, переадресации, несанкционированного ознакомления и (или) уничтожения, ложной авторизации, в том числе аутентификации входных электронных сообщений	1	1	0,5	1	1	1	1	1
4	Технология обработки защищаемой информации обеспечивает взаимную (двухстороннюю) аутентификацию участников обмена электронными сообщениями средствами вычислительной техники соискателя	1	1	0	0	0	1	1	1
5	…….	1	1	0	0	0	1	1	1

04. Раздел 2. Безопасность программного обеспечения

Направление деятельности	Вид деятельности	Вид оценки	Значение оценки
2	3	4	5
№ 683-П	ОПДС	Епоп	0,5
		Епор	0,75
		Епок	0,16
		Епос	1
		Епо	0,59
		ППО ОС	оценка соответствия ОУД

Раздел включает в себя оценку технологических мер положения в соответствии с методикой, изложенной в Приложении 1 к Положению Банка России от 3 декабря 2020 года N 742-П.

Методика расчёта

$$E_{\text{поп}} = \frac{\sum_{i=1}^{N} E_{\text{По}_i} + \sum_{i=1}^{N} E_{\text{Пп}_i}}{2N}, \quad (1)$$

$$E_{\text{пор}} = \frac{\sum_{i=1}^{N} E_{\text{Рм}_i}}{N}, \quad (2)$$

$$E_{\text{пок}} = \frac{\sum_{i=1}^{N} E_{\text{Ко}_i} + \sum_{i=1}^{N} E_{\text{Кп}_i} + \sum_{i=1}^{N} E_{\text{Кз}_i}}{3N}, \quad (3)$$

$$E_{\text{пос}} = \frac{\sum_{i=1}^{N} E_{\text{Си}_i} + \sum_{i=1}^{N} E_{\text{Сн}_i}}{2N}, \quad (4)$$

$$E_{\text{ПО}} = 0{,}2E_{\text{ПОП}} + 0{,}4E_{\text{ПОР}} + 0{,}25E_{\text{ПОК}} + 0{,}15E_{\text{ПОС}}, \quad (5)$$

Раздел 3. 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	№ 683-П	ОПДС	Процесс 1 «Обеспечение защиты информации при управлении доступом»	Епзи1	0,89
				Ер1	0,80
				Еп1	0,82
				Ек1	1,00
				Ес1	1,00
				Еас	0,90
				Уровень соответствия	Четвёртый уровень
				Е1	0,90
			…	…	…

ГОТОВЫ ОТВЕТИТЬ НА ВАШИ ВОПРОСЫ!

Дмитрий Кобец

- Эксперт в сфере информационной безопасности
- Заместитель директора технического департамента **RTM Group**


+7 (495) 197-64-95


info@rtmtech.ru


https://rtmtech.ru


rtm.group


t.me/kurilka_ib