

Разбор проекта изменений в 683-П ЦБ РФ от 9 июня 2021 года

RTM TECHNOLOGIES – первая экспертная компания, специализирующаяся на проведении нормативных и нормативно-технических экспертиз в области ИБ и ИТ.

СОДЕРЖАНИЕ

- 01** Анализ уязвимостей по ОУД4 >> оценка соответствия по ОУД4
- 02** Сертификация на отсутствие НДС >> сертификация по 76 приказу ФСТЭК
- 03** Сертификация для значимых КО и для всех остальных
- 04** Применение СКЗИ
- 05** Технологические меры
- 06** О реагировании (принятых мерах) на инциденты ИБ
- 07** О чем еще информировать ЦБ?
- 08** Сроки реализации

ПРОВЕРЯЮЩАЯ ОРГАНИЗАЦИЯ

«4.2. По решению кредитной организации оценка соответствия программного обеспечения автоматизированных систем и приложений проводится самостоятельно или с привлечением организации, имеющей лицензию на осуществление деятельности по технической защите конфиденциальной информации на проведение работ и услуг, предусмотренных подпунктами «б», «д» или «е» пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации от 3 февраля 2012 года № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» (Собрание законодательства Российской Федерации, 2012, № 7, ст. 863; 2016, № 26, ст. 4049) (далее – проверяющая организация).».

1. ОУД4

Анализ уязвимостей по ОУД4 заменен на оценку соответствия по ОУД4

Оценку соответствия по ОУД4 можно делать самостоятельно либо с привлечением лицензиата ФСТЭК

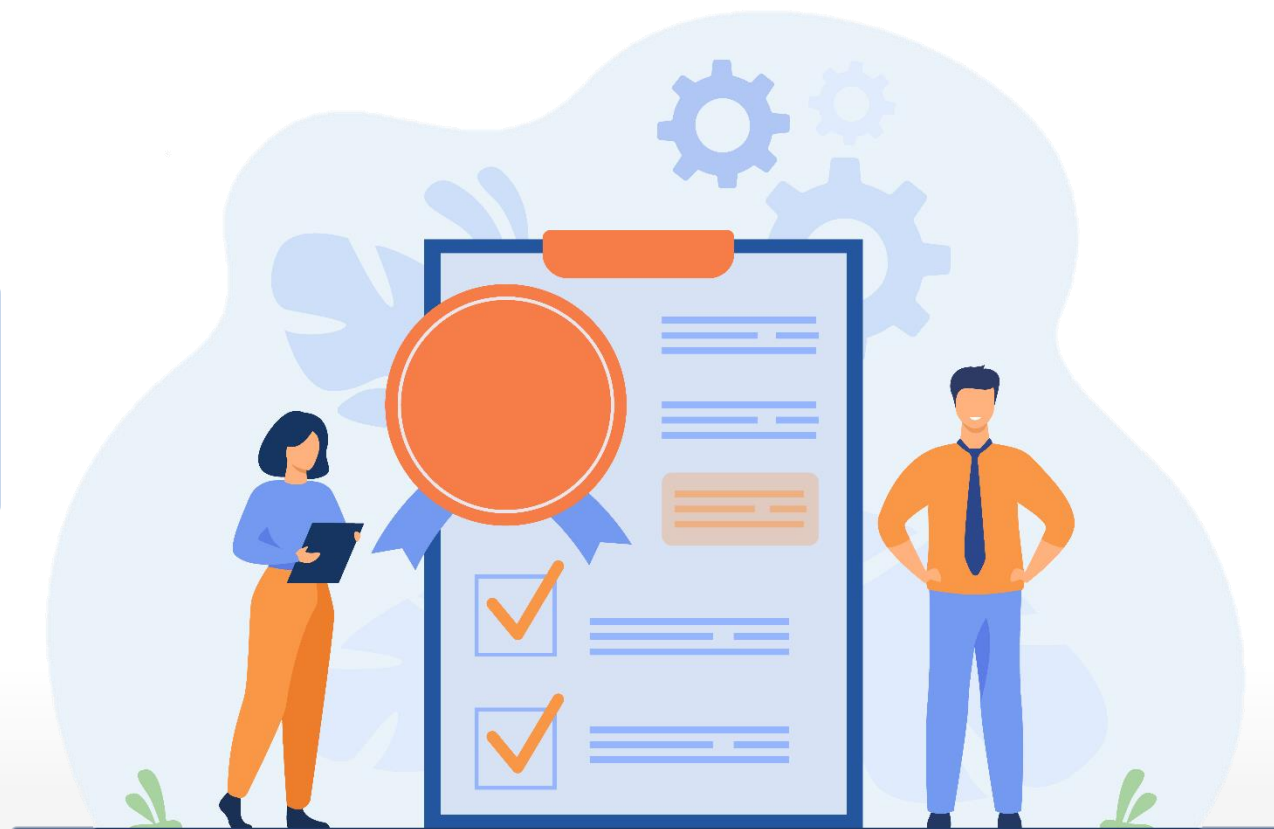


СООТВЕТСТВИЕ / АНАЛИЗ УЯЗВИМОСТЕЙ

Класс доверия	Семейство доверия	Компоненты доверия из оценочного уровня доверия						
		ОУД1	ОУД2	ОУД3	ОУД4	ОУД5	ОУД6	ОУД7
Разработка	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Руководства	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Поддержка жизненного цикла	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Оценка задания по безопасности	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Тестирование	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	2	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Оценка уязвимостей	AVA VAN	1	2	2	3	4	5	5

2. СЕРТИФИКАЦИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Сертификация на отсутствие НДВ
заменена на сертификацию ФСТЭК по
76 приказу.



3. СЕРТИФИКАЦИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Для значимых КО

- Сертификация по 4 уровню доверия

Для остальных КО

- Сертификация по 5 уровню доверия



Решение о сертификации принимается самостоятельно.

4. ПРИМЕНЕНИЕ СКЗИ

Применение СКЗИ – надо применять УКЭП или УНЭП если не используются выделенные каналы связи.



5. ТЕХНОЛОГИЧЕСКИЕ МЕРЫ

Для операций (как совершенных клиентами, так и сотрудниками) необходимо регистрировать ***код банковской операции***.

6. ИНЦИДЕНТЫ ИБ

1

Данные об инцидентах защиты информации передаются в СУР Банка. Передача данных должна быть регламентирована.

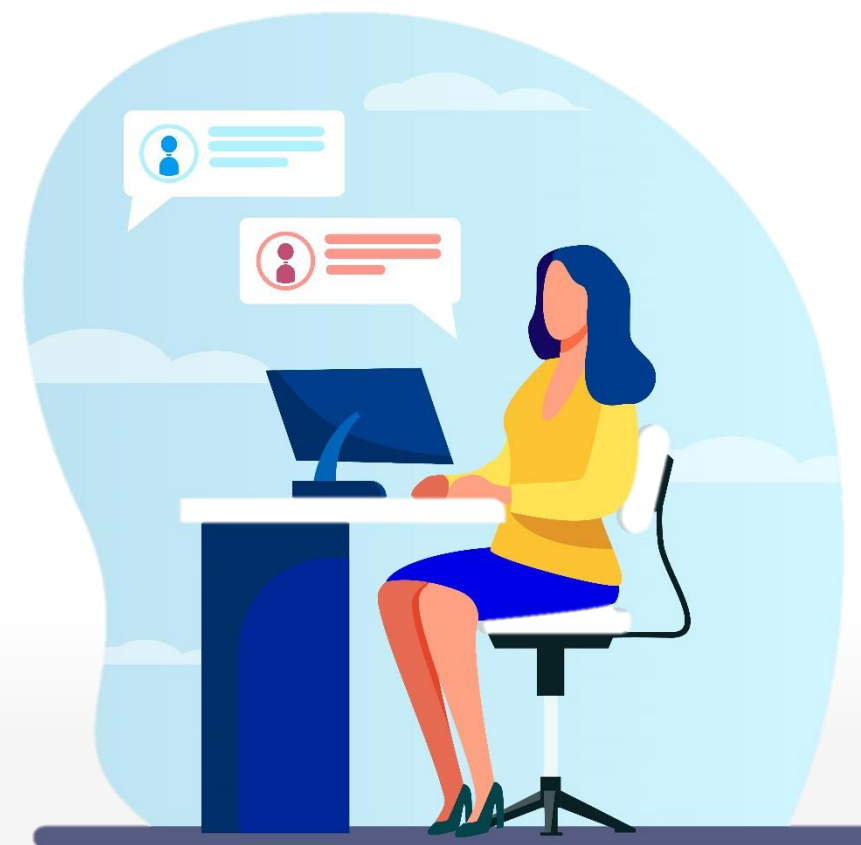
2

Данные о реагировании (принятых мерах) на инциденты ИБ передаются в Банк России.

7. О ЧЕМ ЕЩЕ ИНФОРМИРОВАТЬ ЦБ?

!

Информировать ЦБ о сайтах, при помощи которых осуществляется банковская деятельность (не только о раскрытии информации)



8. СРОКИ РЕАЛИЗАЦИИ

**Вступает (?) в силу
с 01.04.2022 года**



ГОТОВЫ ОТВЕТИТЬ НА ВАШИ ВОПРОСЫ!

Царев Евгений Олегович

Управляющий RTM Group

Музалевский Федор Александрович

Кандидат физико-математических наук

Ведущий судебный эксперт

Директор технического департамента RTM Group



+7 (495) 197-64-95



info@rtmtech.ru



<https://rtmtech.ru>



GroupRTM



rtm.group



@GroupRtm



rtm.group.Russia



t.me/kurilka_ib