



Technologies
Automation
Business.

Обзор изменений в 850-П по сравнению с 787-П

Ключевые изменения:

1. Отдельно выделены требования к иностранным банкам и значимым кредитным организациям
2. Обновлено формулировки в соответствии с изменениями в 716-П и 851-П
3. Отдельно выделено внимание на сотрудников
4. Определено сигнальное время фиксации инцидента ОН как 5 минут от наступления деградации/простоя
5. Определение сигнальных и контрольных значений допустимой доли деградации и времени простоя технологических процессов

1. Введение отдельных требований для значимых КО:

Кредитные организации, признанные значимыми на рынке платежных услуг в соответствии с абзацем шестым пункта 2 Указания Банка России от 6 ноября 2014 года N 3439-У "О порядке признания Банком России кредитных организаций значимыми на рынке платежных услуг» (далее - Указание Банка России N 3439-У), в рамках обеспечения операционной надежности должны обеспечить соблюдение предусмотренных приложением 1 к настоящему Положению значений порогового уровня допустимого времени простоя и (или) деградации технологических процессов для кредитных организаций, признанных значимыми на рынке платежных услуг в соответствии с Указанием Банка России N 3439-У, не позднее шести месяцев с даты признания кредитных организаций значимыми на рынке платежных услуг в соответствии с Указанием Банка России N 3439-У.

2. Расширение описания обеспечения операционной надежности

Кредитные организации должны обеспечить операционную надежность <...> при:

787-П: возникновении отказов и (или) нарушений функционирования объектов информационной инфраструктуры, и (или) несоответствии их функциональных возможностей и характеристик потребностям кредитной организации (далее - сбой объектов информационной инфраструктуры), и (или) реализации киберриска, предусмотренного абзацем вторым пункта 7.2 Положения Банка России № 716-П.

850-П: возникновении отказов и (или) нарушений функционирования объектов информационной инфраструктуры, и (или) несоответствии их функциональных возможностей и характеристик потребностям кредитных организаций, филиалов иностранных банков (далее - сбой объектов информационной инфраструктуры);

реализации риска преднамеренных действий со стороны работников кредитной организации, филиала иностранного банка и (или) третьих лиц с использованием программных и (или) программно-аппаратных средств, направленных на объекты информационной инфраструктуры кредитной организации, филиала иностранного банка в целях нарушения и (или) прекращения их функционирования, и (или) создания угрозы безопасности информации, подготавливаемой, обрабатываемой и хранимой такими объектами, а также в целях несанкционированного присвоения, хищения, изменения, удаления данных и иной информации (структуры данных, параметров и характеристик систем, программного кода) и нарушения режима доступа.

3. Фокус на сотрудников

Кредитные организации, филиалы иностранных банков должны принимать меры, направленные на нейтрализацию угроз в отношении возникновения зависимости обеспечения операционной надежности от работников кредитных организаций, филиалов иностранных банков, обладающих уникальными знаниями, опытом и компетенцией в области разработки технологических процессов, поддержания их выполнения, реализации технологических процессов, которые отсутствуют у иных работников указанных кредитных организаций, филиалов иностранных банков.

Кредитные организации, филиалы иностранных банков должны обеспечить защиту критичной архитектуры от возможной реализации информационных угроз в условиях дистанционной (удаленной) работы работников кредитных организаций, филиалов иностранных банков.

4. Пять минут

Кредитные организации с соблюдением требований главы 5 Положения Банка России N 716-П должны установить для каждого технологического процесса и соблюдать сигнальные и контрольные значения, предусмотренные пунктом 5.1 Положения Банка России N 716-П, для следующих контрольных показателей уровня операционного риска для целей обеспечения операционной надежности (далее - показатели операционной надежности):

787-П: допустимого времени простоя и (или) деградации технологических процессов кредитных организаций в рамках инцидента операционной надежности (в случае превышения допустимой доли деградации технологического процесса). Значение данного целевого показателя устанавливается кредитной организацией не выше значений, предусмотренных приложением к настоящему Положению;

850-П: допустимого времени простоя и (или) деградации технологических процессов кредитных организаций в рамках инцидента операционной надежности (в случае несоблюдения в течение временного периода, превышающего пять минут, сигнального значения допустимой доли деградации технологического процесса);

4. Пять минут

850-П: В случаях несоблюдения в течение временного периода, превышающего пять минут, сигнального значения допустимой доли деградации технологических процессов кредитные организации должны фиксировать:

фактическое время простоя и (или) деградации технологического процесса, исчисляемое по каждому инциденту операционной надежности (с момента нарушения технологического процесса, приводящего к неоказанию или ненадлежащему оказанию банковских услуг, в связи с возникновением события или серии связанных событий, вызванных информационными угрозами и (или) сбоями объектов информационной инфраструктуры, до момента восстановления технологического процесса);

фактическую долю деградации технологического процесса в рамках отдельного инцидента операционной надежности;

суммарное время простоя и (или) деградации технологического процесса за последние двенадцать календарных месяцев.

5. Определение значений допустимого времени простоя (Приложение 1)

Контрольное значение показателя допустимого времени простоя/деградации устанавливается кредитными организациями не выше значений, предусмотренных приложением 1 к настоящему Положению.

N п/п	Наименование технологического процесса	Пороговый уровень допустимого времени простоя и (или) деградации технологических процессов (в часах)				
		для банка > 500 миллиардов рублей	для банка < 500 миллиардов рублей	для банка с базовой лицензией	для небанковской кредитной организации	для филиала иностранного банка
1	2	3	4	5	6	7
1	ТПРКО1	2	4	6	X	X
2	ТПРКО2	2	4	6	6	X
3	ТПРКО3	2	4	6	6	X
4	ТПРКО4	2	2 - для значимых КО по N 3439-У	2 - для значимых КО по N 3439-У	X	X
5	ТПРКО5	2	2 - для значимых КО по N 3439-У	2 - для значимых КО по N 3439-У	2 - для значимых КО по N 3439-У	4
6	ТПРКО6	2	2	2	X	X
7	ТПРКО7	2	2	2	2	2
8	ТПРКО8	2	2 - для значимых КО по N 3439-У	2 - для значимых КО по N 3439-У	2 - для значимых КО по N 3439-У	4
9	ТПРКО9	24	24	24	X	X
10	ТПРКО10	2	2	2	X	2
11	ТПРКО11	2	2	2	X	2
12	ТПРКО12	2	2	2	X	X
13	ТПРКО13	2	2	2	X	X

5. Определение значений допустимой доли деградации (Приложение 2)

При установлении сигнального и контрольного значений допустимой доли деградации технологического процесса кредитные организации должны установить сигнальное и контрольное значения не ниже значений, предусмотренных приложением 2 к настоящему Положению.

N п/п	Наименование технологического процесса	для банка, размер активов которого составляет 500 миллиардов рублей и более		для банка с универсальной лицензией, размер активов которого составляет менее 500 миллиардов рублей		для банка с базовой лицензией		для небанковской кредитной организации	
		сигнальное значение (в долях)	контрольное значение (в долях)	сигнальное значение (в долях)	контрольное значение (в долях)	сигнальное значение (в долях)	контрольное значение (в долях)	сигнальное значение (в долях)	контрольное значение (в долях)
1	2	3	4	5	6	7	8	9	10
1	ТПРКО1	0,90	0,80	0,87	0,75	0,85	0,70	X	X
2	ТПРКО2	0,90	0,80	0,87	0,75	0,85	0,70	0,75	0,50
3	ТПРКО3	0,90	0,80	0,87	0,75	0,85	0,70	0,75	0,50
4	ТПРКО4	0,90	0,80	0,87	0,75	0,85	0,70	X	X
				0,90 - для значимых КО по N 3439-У	0,80 - для значимых КО по N 3439-У	0,90 - для значимых КО по N 3439-У	0,80 - для значимых КО по N 3439-У		
5	ТПРКО5	0,90	0,80	0,87	0,75	0,85	0,70	0,75	0,50
				0,90 - для значимых КО по N 3439-У	0,80 - для значимых КО по N 3439-У	0,90 - для значимых КО по N 3439-У	0,80 - для значимых КО по N 3439-У	0,90 - для значимых КО по N 3439-У	0,80 - для значимых КО по N 3439-У
6	ТПРКО6	0,92	0,85	0,90	0,80	0,87	0,75	X	X
7	ТПРКО7	0,92	0,85	0,90	0,80	0,87	0,75	0,75	0,50
8	ТПРКО8	0,90	0,80	0,87	0,75	0,85	0,70	0,75	0,50
				0,90 - для значимых КО по N 3439-У	0,80 - для значимых КО по N 3439-У	0,90 - для значимых КО по N 3439-У	0,80 - для значимых КО по N 3439-У	0,90 - для значимых КО по N 3439-У	0,80 - для значимых КО по N 3439-У
9	ТПРКО9	0,90	0,80	0,90	0,80	0,90	0,80	X	X
10	ТПРКО10	0,92	0,85	0,90	0,80	0,87	0,75	X	X
11	ТПРКО11	0,92	0,85	0,90	0,80	0,87	0,75	X	X
12	ТПРКО12	0,92	0,85	0,90	0,80	0,87	0,75	X	X

Ответы на вопросы

Вопрос:

Если в организации критерий регистрации СОР ИС зафиксирован как превышение сигнального значения допустимой доли деградации в течение 30 минут, то значит ли это, что мы можем не регистрировать ИОН длительностью менее 30 минут, так как он прежде всего не является для нас СОРом ИС?

850-П:

«Кредитные организации должны информировать Банк России:
о выявленных инцидентах операционной надежности (в случае несоблюдения в течение временного периода, превышающего пять минут, сигнального значения допустимой доли деградации технологических процессов) кредитных организаций, а также о принятых мерах и проведенных мероприятиях по реагированию на выявленный кредитными организациями или Банком России инцидент операционной надежности <...>»

Вывод: В новом тексте положения точка отсчета, после которой инцидент подлежит сообщению в ЦБ, определена как «несоблюдение допустимой доли деградации в течении периода, превышающего пять минут».



Стоимость лицензий: **180 тыс руб¹**

Поддержка: 180 тыс руб./год

- Первая версия вышла в 2018 году.
- Лидер рынка среди отечественного ПО, более 300 внедрений.
- Отечественное ПО, разработано на базе 1С:Предприятие (дополнительно устанавливаемое расширение).
- Решение может быть развернуто на защищенной платформе 1С:Предприятие 8.3z, которая имеет сертификацию ФСТЭК 4-го уровня доверия.
- Открытый исходный код – удобство для самостоятельной поддержки решения после внедрения и его развития.
- Соответствует спецификации GRC.
- Решение соответствует следующим требованиям и стандартам:
 - 208-ФЗ, 259-ФЗ и проект нормоакта для ЦФА
 - Указания Банка России 4501-У и 5683-У
 - Положения Банка России 779-П, 757-П, 716-П, 744-П, 787-П, 781-П
 - ISO 31000, COSO 2017
 - Требования НСПК

¹ Стоимость представлена со всеми налогами, НДС не облагается

Присоединяйтесь к нам в социальных сетях



Telegram



ВКонтакте



RUTUBE

Благодарим за внимание!

TAB | Technologies
Automation
Business.

ООО «Технологии и бизнес»

105318, г. Москва, ул. Вельяминовская,
д.9, эт./ком. 5/32

Тел/факс: +7 (495) 128 13 54
Email: sales@businesstech.store

8-800-600-64-10 (во всех регионах РФ
БЕСПЛАТНО)
<https://businesstech.store>

*С уважением к Вам
и Вашему бизнесу*

TAB | Технологии
Автоматизация
Бизнес