deiteriy compliance

Управление рисками ИБ в ПС «Мир»

АЛЕКСАНДР ИВАНЦОВ | DEITERIY COMPLIANCE | конференция АБИСС 2025, МОСКВА

Александр Иванцов

Старший инженер по защите информации
Deiteriy Compliance
aleksandr.ivantsov@deiteriy.com
+7 (911) 785-97-96

Требования НСПК по управлению рисками ИБ

Стандарт ПС «Мир». Требования к системе управления Рисками информационной безопасности Субъектов ПС «Мир».

- Необходимо заниматься управлением рисками ИБ
- Необходимо проводить оценку эффективности системы управления риском ИБ и отчитываться перед НСПК

Цели требований

- Удовлетворение требований ЦБ
- Контроль за уровнем ИБ поднадзорных организаций (но не по AOC и ROC по результатам QSA аудитов)

Требования НСПК по управлению рисками ИБ

Этап	Когда?
Выявление, идентификация, анализ и оценка рисков ИБ	**1 раз в год**
Оценка эффективности функционирования системы управления Риском ИБ	**1 раз в 2 года**
Мониторинг рисков ИБ	**Постоянно**

Оценка рисков ИБ

Воздействие						
	5	В	В	К	К	К
	4	С	С	В	В	В
	3	Н	С	С	С	С
	2	Н	Н	Н	Н	С
	1	Н	Н	Н	Н	Н
		1	2	3	4	5
		Вероятность				

Управление рисками ИБ не в вакууме

Правила НСПК

Выявление, идентификация, анализ и оценка рисков ИБ

PCI DSS

Ежегодный TRA (Targeted Risk Analysis)

716-П

Ежегодная самооценка операционного риска

Оценка эффективности функционирования СУР ИБ

- Полностью охватывает как методику оценки рисков и адекватность принятых мер снижения риска, так и этапы мониторинга рисков и совершенствование СУР
- Должна быть независимой: проводит СВА или внешний аудитор
- Результаты фиксируются отчетом, который утверждается руководством (или лицами, принимающими решения по вопросам ИБ)

Что изменилось в оценке эффективности?

- Определены базовые и ключевые критерии
- Определена методика оценки
- Описаны приемлемые свидетельства
- Шаблонизирован отчет по результатам проведения процедуры

Мониторинг - постоянный процесс

Метрики эффективности системы управления рисками ИБ

Контрольные показатели уровня операционного риска (КПУР) – глобальные показатели, установленные для организации (процесса) в целом. Используются в целях контроля процесса управления операционными рисками и выявления глобальных проблем.

Метрики эффективности системы управления рисками ИБ

Ключевые индикаторы риска (КИР) – индикаторы, установленные для каждого риска в отдельности. Используются в целях обнаружения факта реализации риска.

Метрики эффективности системы управления рисками ИБ

КИР	КПУР
Устанавливаются для каждого риска	Устанавливаются глобально для организации Часть уже выбрана НСПК
Нужно придумать пороговые значения	Нужно придумать сигнальные и контрольные пороговые значения
Нужно придумать порядок реагирования на превышение порога	Порядок реагирования определен за нас
Устанавливается периодичность мониторинга, производится расчет	Устанавливается периодичность мониторинга, производится расчет Выбранные НСПК КПУР нужно мониторить ежеквартально
Ежегодный пересмотр	Ежегодный пересмотр

Порядок реагирования на сигнальные и контрольные значения КПУР (716-П)

Сигнальные	Контрольные
Ежедневный мониторинг	Сообщение совету директоров
	Дополнительные придуманные и задокументированные меры

Правила НСПК позволяют определить свой набор уровней и их градаций.

Какие КПУР для нас приготовили?

- Сумма ущерба от инцидентов, связанных с переводами по картам
- Сумма ущерба от инцидентов, которые привели к несанкционированным операциям с использованиям карт эмитированных организацией
- Отношение ущерба от инцидентов к общему объему операций, прошедших через компанию
- Отношение количества инцидентов с ущербом к общему количеству инцидентов ИБ

Какие КПУР для нас приготовили?

- Сумма ущерба от инцидентов у третьих лиц
- Отношение количества подтвержденных инцидентов к неподтвержденным инцидентам ИБ у третьих лиц
- Сравнение количества инцидентов с прошлым годом
- Показатели опернадежности

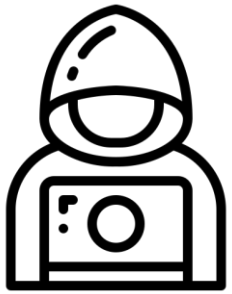
Какие КПУР для нас приготовили?

- Оценка эффективности СУР (раз в 2 года)
- Оценка эффективности защитных мер, применяемых по требованиям Программы безопасности ПС «МИР»
- Оценка эффективности компенсационных мер для требований PCI DSS

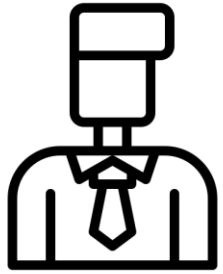
Мониторинг - постоянный процесс

Показатели, связанные с PCI DSS – не раз в год, а как минимум раз в квартал.

Кто должен этим заниматься?



ИБ	Риски
Выявление инцидентов Сбор информации Регистрация инцидента Оценка потерь	Регистрация события операционного риска Фиксирование количественных и качественных потерь
Оценка рисков ИБ	Оценка эффективности СУР
Контрольные следы по результатам выполнения процедур	Мониторинг КПУР



Что попросит НСПК?

- Перечень рисков и их оценки
- Установленные значения КПУР
- Выбранные КИР и их пороговые значения
- Результаты оценки эффективности СУР
- Методики расчета

Формализация и шаблонизация процесса

«+»

Процедура стала проще и понятнее, выполнение требует меньше трудозатрат и меньших разбирательств в «правилах».

«-»

Переход от «духа» к «форме». Есть соблазн «научиться правильно заполнять» вместо того чтобы выполнять исходную задачу.

Выводы

1. Регулятор читает, что ему присылают

2. Не расслабляемся – если результат приняли, это не значит, что всё в порядке

3. Следуем здравому смыслу и не забываем о целях

Спасибо за внимание!