ТАБ Технологии Автоматизация Бизнес

Обзор требований НСПК. Часть 2.

Презентационные материалы к вебинару

Москва, 2025 г.

Содержание вебинара


МИР

Вводится в действие с 04.09.2023

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

П.255

Версия 1.1

НСПК
Москва, 2023

1. Требования стандарта НСПК по рискам ИБ

2. Соответствие к требованиям 716-П (гармонизация)

3. Базовая теория управления рисками

Регуляторное окружение

- Требования НСПК

Еще большая конкретизация подходов

- 716-П
- 850-П
- и т.д.

Конкретизация подходов

- ГОСТ 31000
- COSO 2017
- GRC
- и т.д.

Принципы

Технологии
Автоматизация
Бизнес

Требования стандарта НСПК

Требования стандарта НСПК

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

Оглавление

Статья с базовой информацией про риск ИБ

Требования к обеспечению защиты информации

*4.8 Субъект **должен** составлять Профили Рисков ИБ. Рекомендации по формированию **Профиля Рисков ИБ** приведены в Приложении № 1 настоящего документа.*

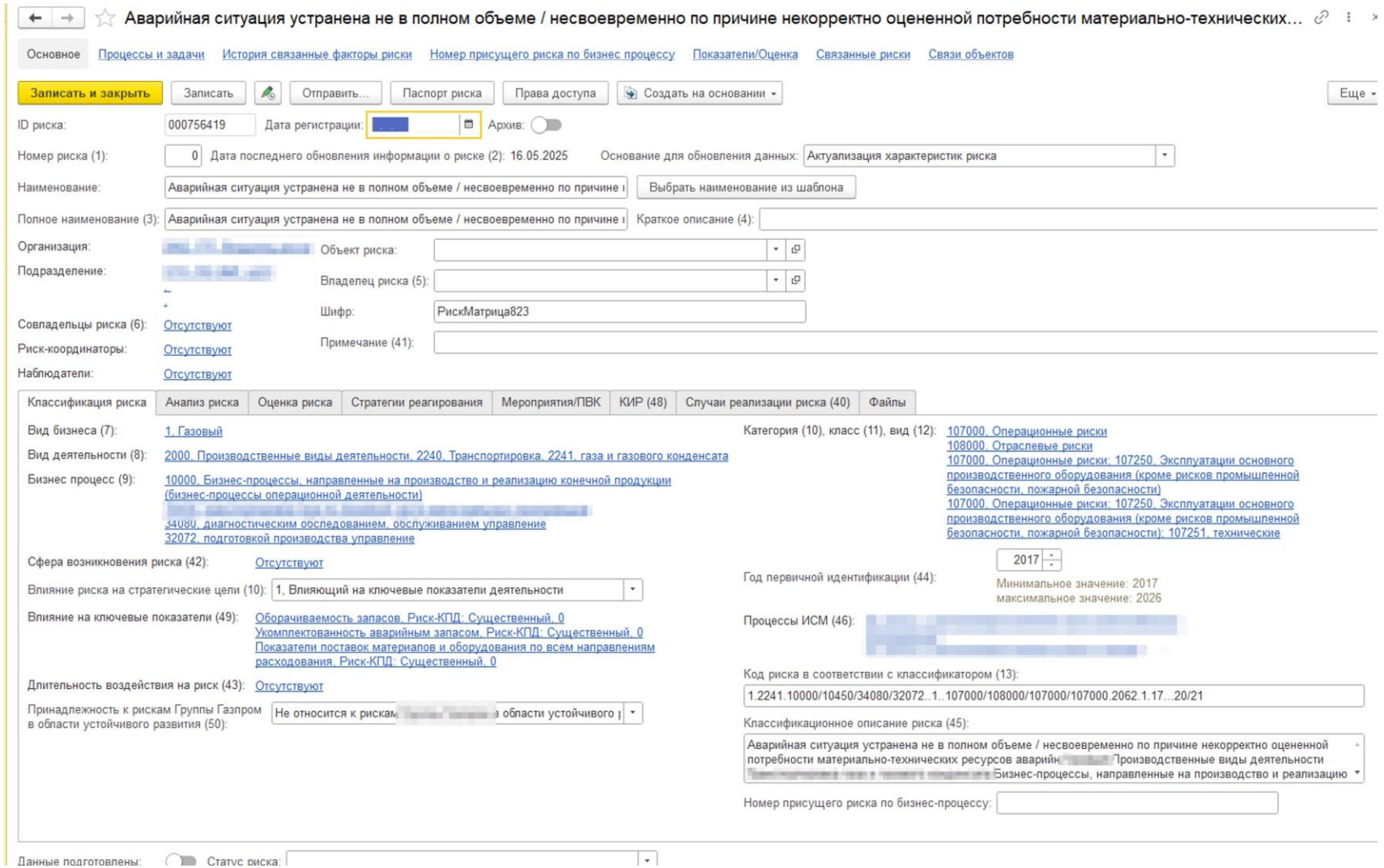
Прил.1 Рекомендации по формированию профиля Рисков ИБ

***Рекомендуется** включать в профиль Рисков ИБ подробное описание каждого Риска ИБ с указанием следующей информации:*

- *описание бизнес-процессов, в которых могут произойти Риск-события; (прим. эмиссии карт нет в списке техпроцессов)ы*
- *перечень объектов информационной инфраструктуры, на которые влияет Риск- событие;*
- *описание Риск-события;*
- *описание причины (источник) возникновения Риск-события;*
- *вероятность наступления Риск-события;*
- *описание и оценка возможных неблагоприятных последствий Риск-события;*
- *уровень Риска (присущий, допустимый, остаточный);* (прим. значение также должно быть)
- *перечень способов управления Риском.*

Требования к обеспечению защиты информации

Технологии Автоматизация Бизнес

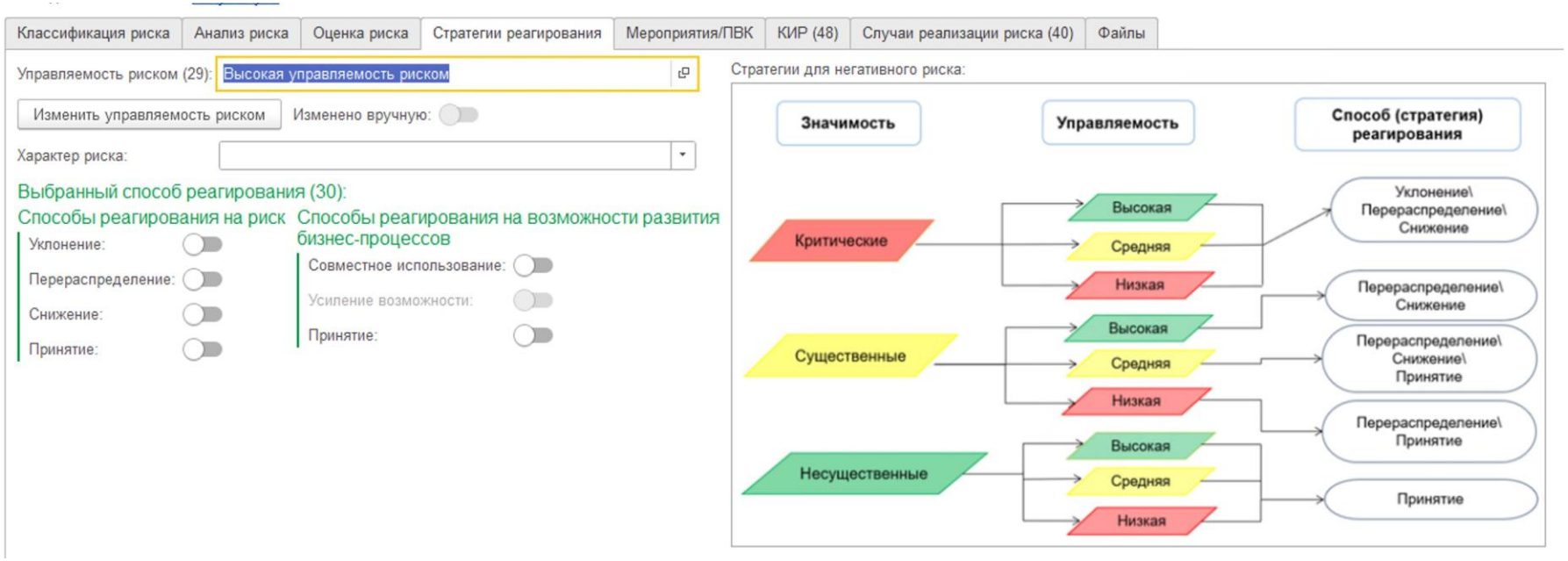


Пример профиля риска в информационной системе

Профиль риска = паспорт риска

Требования к обеспечению защиты информации

Технологии Автоматизация Бизнес



Пример профиля риска в информационной системе

Профиль риска = паспорт риска

Требования к обеспечению защиты информации

ПАСПОРТ РИСКА: XX					
Наименование процесса				Управление закупками	
Уровень риска (значительный/критический)				Значительный	
Ответственный				Руководитель отдела закупок	
Общая информация о риске					
Наименование риска				Неспособность обеспечить 100% соответствие плану закупок	
Причины				Некорректный выбор поставщиков	
Последствия риска				Срыв планируемой деятельности	
Критическая точка				Информация по количеству претензий к выбранному списку поставщиков на дату XX.XX.XXXX	
№	Мероприятия по снижению/оптимизации уровня риска (ресурсы)			Ответственный	
1	Ведение записей по анализу поставщиков			Руководитель отдела закупок	
Реализация риска					
№	Дата	Наименование события	Причина	Корректирующие мероприятия. Коррекция	Комментарии
1	10.01.XX	Срыв поставки	Не проверенный поставщик	Внесен в базу «черного списка»	Нет
Оценка остаточного риска (30.10.XX) (предполагаемая после выполнения всех мероприятий)					
С введением процедуры оценки поставщиков данный риск перешел в зону «приемлемости» - и имеет оценку 4					

Пример профиля риска в эксель форме

Можно найти форму паспорта риска в интернете

Требования к обеспечению защиты информации

Технологии Автоматизация Бизнес

Несколько особенностей:

1. Профилей рисков – в среднем 500-5000 записей.

2. Шаблон наименования: _____ (последствие) вследствие ____ по причине _____ с последующим ____

Пример:
Остановка работы платежной системы в следствие DDOS-атаки на ресурсы организации по причине начала широкой рекламной компании на розничного потребителя с последующим подъемом социального напряжения в обществе.

3. Детализация может быть любой: от верхнеуровневой, до очень детальной.

4. Профиль обычно явно связан с КИРами для него. Но в требованиях нет связи явной.

Требования к обеспечению защиты информации

5. Требования к обеспечению защиты информации

5.1. Субъекты должны выполнять требования по обеспечению защиты информации, установленные в документе [2], ***в отношении выявленных и идентифицированных Рисков ИБ*** *в ПС «Мир». (*прим. 1. Не выявлено – не применяем меры 2. Мера всегда привязана к риску*)*

5.2 ***В случае недостаточности*** *защитных мер, реализованных в соответствии с требованиями документа [2], для минимизации* (прим. компенсирующие меры) *выявленных и идентифицированных Рисков ИБ Субъекта, Субъект должен* ***самостоятельно*** *определить и реализовать* ***дополнительные защитные меры****, в дополнение к требуемым документом [2].*
(прим. Если меры реализованные по стандарту [2] по мнению экспертов компании не привели к снижению остаточного риска ниже допустимого, то еще чтото придумываем и реализуем)

[2] Стандарт ПС «Мир». Программа безопасности.

6. Инциденты ИБ

6.1. Управление Инцидентами ИБ должно выполняться с учетом требований, установленных в ПС «Мир» (см. документ [3]).

[3] Стандарт ПС «Мир». Порядок обработки инцидентов ИБ Участником

Оценка эффективности функционирования системы управления Риском ИБ

7. Оценка эффективности функционирования системы управления Риском ИБ

7.1. Субъект должен ***самостоятельно*** (прим. службой вн.аудита) *проводить оценку эффективности системы управления Рисками ИБ в рамках своей деятельности в ПС «Мир», в том числе* ***оценку*** *используемых методов* ***оценки*** *и анализа Рисков ИБ,* ***результатов применения способов управления*** *Рисками ИБ.*
7.2. Оценка должна проводиться не реже ***одного раза в два года.***
7.3. Субъект должен ***самостоятельно*** *установить* ***критерии*** *эффективности своей системы управления Рисками ИБ.* (прим. документарно в регламенте)
7.4. В случае ***признания системы*** *управления Рисками ИБ* ***эффективной****,* ***мероприятия*** *по минимизации Рисков ИБ также считаются* ***эффективными****.*
7.5. В случае если система управления Рисками ИБ за анализируемый период признана ***неэффективной****, Субъект* ***должен*** *разработать* ***новые меры*** *для достижения и поддержания* ***остаточного уровня*** *Рисков ИБ* ***не выше допустимого*** *уровня Рисков ИБ, либо установить новые допустимые уровни Рисков ИБ Субъекта.*

Это внутренний аудит
3я линия защиты

Последний вебинар НСПК был на тему именно данной главы 7. То есть, направлен не на ИБ, а на внутренних аудиторов

Задача аудитора:

1. Верно ли оценен риск?
2. Все ли риски идентифицированы? (явно не указано)
3. Разработанные меры действительно ли снижают риск?

Оценка эффективности функционирования системы управления Риском ИБ

7.6. Результат оценки эффективности системы управления Риском ИБ ***должен*** *быть оформлен* ***документально****. Рекомендации по содержанию отчетной документации, содержащей результаты оценки приведены в Приложении № 1 настоящего документа.*

В отчетную документацию рекомендуется включать следующую информацию:

- *описание* ***методов*** *оценки и анализа Рисков ИБ;*
- *результаты* ***мониторинга*** *Рисков ИБ;* (прим. Фактические значения показателей ПУР, даже без из нарушений)
- *описание* ***используемых мер минимизации*** *Рисков ИБ;* (прим. компенсирующие меры)
- ***результаты*** *применения* ***способов управления*** *Рисками ИБ;* (прим. результаты компенсирующих мер или страхования, резервирования и тд)
- ***результаты оценки эффективности*** *функционирования системы управления Риском ИБ Субъекта.* (прим. общая оценка аудитора по результатам проверки)

Оценка эффективности функционирования системы управления Риском ИБ

Технологии Автоматизация Бизнес

7.7. Результат оценки должен быть ***утвержден уполномоченным*** *органом Субъекта, у которого есть полномочия по рассмотрению/утверждению* ***вопросов оценки эффективности*** *системы управления рисками.* (прим. по умолчанию совет директоров/наблюдательный совет, если не указано в Уставе или других документах подписанных на уровне СД/НС/акционеров. Тут редкий случай, когда это не относится к компетенции правления).

7.8. Субъект ***должен по запросу*** *предоставлять в АО «НСПК»* ***отчетную документацию с результатами оценки эффективности*** *системы управлении Рисками ИБ Субъекта в* ***сроки*** *и в порядке, установленном в таком* ***запросе.***

Мониторинг Риска ИБ

8. Мониторинг Риска ИБ

8.1. Субъект должен осуществлять ***мониторинг*** *Рисков ИБ в целях своевременного выявления ситуаций, требующих принятия* ***мер реагирования***. (прим. периодическое отслеживание показателей уровня риска, в целях управления организацией)

8.2. Мониторинг должен осуществляться путем отслеживания показателей уровня Рисков ИБ. (прим. Вводится термин **ПУР**, аналоги - КИР, КПУР)

Суть мониторинга рисков

Цель мониторинга – установить контрольные точки, требующие реакции

КИР/ПУР/КПУР – установленное к мониторингу число

Мониторинг многоуровневый, но мы применяем три уровня:

1. Реакция руководителя (1я линия)
2. Реакция риск-менеджера (2я линия)
3. Реакция регулятора (внешняя линия)

Примеры:

- Среднее время обработки платежа < 500 мс
- Остановка системы в течение 1 часа < 1 мин
- Уязвимости (CVSS ≥7.0) > 48 часов без патча
- Результат аудита по ГОСТ 57580.2 < 85%

Суть мониторинга рисков

КИР – «сырой» чистый показатель

ПУР – индикативный обобщенный показатель

Переменные расчета ПУР – это КИР

ПУР:

общая сумма валовых прямых потерь и сумм величин косвенных потерь Участника в результате наступления Инцидентов ИБ, связанных с осуществлением переводов денежных средств в ПС «Мир»

КИРы:

1. Сумма валовых потерь
2. Сумма прямых потерь
3. Сумма косвенных потерь

ПУР = КИР1 + КИР2 + КИР3

Суть мониторинга рисков

Риск-ориентированный надзор - Это метод регулирования и контроля, при котором интенсивность и частота проверок со стороны регулятора зависят от уровня рисков, связанных с деятельностью поднадзорной организации.

Мониторинг КИР (ПУР/КПУР):

1. Сокращает количество отчетов поднадзорной организации
2. Снижает расходы финансового рынка за счет возможности неисполнения некритичных для бизнеса требований
3. Увеличивает роль службы внутреннего контроля
4. Требует развитой культуры риск-менеджмента

Внешний вид панели управления

Технологии
Автоматизация
Бизнес

Законодательных нарушений

Нет данных для отображения

Прямые потери

9 071 391
-15.23%

Аудиты внешние

6
-14.29%

Аудиты внутренние

7
-30%

Эффективность мер воздействия

25,6162%

Структура предприятия

Ссылка
Департамент закупок и логистики
Департамент закупок и логистики
Управление закупок
Управление запасов
Управление логистики
Департамент защиты активов
Департамент защиты активов
Управление безопасности
Департамент поддержки бизнеса
Департамент правовой и корпоративной...
Департамент продаж
Департамент производства
Департамент производства
Отдел контроля качества
Проектное управление
Производственно-технический отдел
Производственный участок № 1
Производственный участок № 2

Показатели эффективности

Год, Квартал	2024 г. 1 кв.		2024 г. 2 кв.		2024 г. 3 кв.		2024 г. 4 кв.	
Целевой показатель	Стату	Тренд	Стату	Тренд	Стату	Тренд	Стату	Тренд
Выручка организации	●	–	●	↓	●	↑	●	↓
Качество услуг	●	–	●	–	●	–	●	–
Эффективность производства	●	–	●	↑	●	↓	●	↑

План - факт

Ключевые индикаторы риска (КИР)

Год, Квартал	2024 г. 1 кв.		2024 г. 2 кв.		2024 г. 3 кв.		2024 г. 4 кв.	
Показатель	Стату	Тренд	Стату	Тренд	Стату	Тренд	Стату	Тренд
Штрафы от регуляторов	●	–	●	↓	●	↓	●	↑
Происшествия на объектах	●	–	●	↓	●	↑	●	↓
Размер DDoS-атак	●	–	●	–	●	↓	●	↑

План факт (таблица)

План	26 144
Факт	24 415,2
Отклонение	1 728,8
Отклонение, %	-6,6126

Мониторинг Риска ИБ

8.3. Участник должен самостоятельно установить значения для следующих показателей уровня Риска ИБ:

- *показатели, характеризующие **уровень потерь** в результате наступления **Инцидентов ИБ** у Участника:*

*- общая сумма **валовых прямых** потерь и сумм величин **косвенных** потерь Участника в результате **наступления** Инцидентов ИБ, связанных с осуществлением переводов денежных средств в ПС «Мир», за отчетный период (первый квартал, полугодие, девять месяцев, год) **нарастающим итогом** с начала календарного года;*
*- общая сумма **валовых прямых** потерь и сумм величин **косвенных** потерь Участника в результате **наступления** Инцидентов ИБ, которые привели к Несанкционированным операциям с использованием Карт, эмитированных Участником, за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года;*
*- **отношение** суммы **валовых прямых** потерь, понесенных организацией при выполнении функций Участника, за отчетный период (первый квартал, полугодие, девять месяцев, год) **нарастающим итогом** с начала календарного года, к **общей сумме операций переводов** денежных средств Участником в ПС «Мир» за этот же период;*
*- **доля** реализованных **(по количеству) Инцидентов** ИБ с **ненулевой** величиной валовых прямых потерь по отношению **ко всем Инцидентам ИБ** в течение отчетного периода (первого квартала, полугодия, девяти месяцев, года);*

Мониторинг Риска ИБ

Технологии Автоматизация Бизнес

- *показатели, характеризующие **уровень потерь** в результате наступления Инцидентов ИБ у третьих лиц, привлеченных Участником для осуществления деятельности в ПС «Мир»:*

*- общая сумма **валовых прямых** потерь и **косвенных** потерь Участника в результате Инцидентов ИБ у третьих лиц, привлеченных Участником для осуществления деятельности в ПС «Мир», за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года;*

*- **доля подтвержденных** (по **количеству**) Инцидентов ИБ по отношению к **неподтвержденным** Инцидентам ИБ у третьих лиц, привлеченных Участником для осуществления деятельности в ПС «Мир», в течение отчетного периода (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года;*

*- **разница** между **количеством** Инцидентов ИБ **у третьих лиц**, привлеченных Участником для осуществления деятельности в ПС «Мир», за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала **текущего** календарного года и **количеством** Инцидентов ИБ **у третьих лиц**, привлеченных Участником для осуществления деятельности в ПС «Мир», за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала **предыдущего** календарного года;*

Мониторинг Риска ИБ

- *показатели, характеризующие уровень **операционной надежности** процессов в результате наступления **Инцидентов ИБ*** (прим. В 787-П событие опер.риска, а не инцидент)*:*

*- **доля** деградации **бизнес- и технологических процессов**, обеспечивающих осуществление Операций;*

*- **время простоя** и (или) деградации **бизнес- и технологического** процесса (в случае отклонения от контрольного значения доли деградации процессов);* (прим. Реестр «бизнес-процессы» вводится 7-МР по ГОСТ 57580.4)

Мониторинг Риска ИБ

- *показатели, характеризующие* ***уровень зрелости процессов*** *защиты информации:*

- оценка эффективности *функционирования системы управления Риском ИБ,* ***проведенная уполномоченным подразделением*** *и (или)* ***внешним экспертом*** *(специализированной организацией или квалифицированным внешним экспертом) по решению уполномоченного органа Субъекта;* (прим. Внуренний аудит обязателен по 242-П, внешний эксперт если нет компетенций. Уполномоченный орган по-умолчанию – СД/НС).

- оценка эффективности *защитных мер, применяемых в соответствии с требованиями безопасности, определенных для данного Субъекта в соответствии с документом [2] за отчетный период (первый квартал, полугодие, девять месяцев, год) с начала календарного года;*

- оценка эффективности *компенсационных мер, применяемых* ***для достижения целей требований PCI DSS*** *за отчетный период (первый квартал, полугодие, девять месяцев, год) с начала календарного года;* (прим. почему-то ссылка не на [2], регулирующий защитные меры и задачи, а на PCI DSS)

- оценка эффективности *дополнительных защитных мер, в дополнение к мерам, требуемым документом [2], применяемых для обеспечения защиты информационных систем и процессов, используемых для проведения Операций, за отчетный период (первый квартал, полугодие, девять месяцев, год) с начала календарного года.*

«Оценка эффективности» – это всегда про внутренний аудит (3я линия)!

Мониторинг Риска ИБ

*8.4. **ОПКЦ самостоятельно** устанавливает перечень показателей уровня Риска ИБ и значения для показателей уровня Риска ИБ. При выполнении НСПК роли ОПКЦ, показатели определяются НСПК в соответствии с внутренними процессами.*
*8.5. **РЦ самостоятельно** устанавливает значения для показателей уровня Риска ИБ. Перечень показателей уровня Риска ИБ определяется в соответствии с установленным порядком взаимодействия между Оператором и РЦ.*

*8.6. Для каждого показателя уровня Риска ИБ **должно** быть установлено:*

- *шкала оценки показателя;* (прим. Например: 0-1 доля, 1-5 оценка и тд)

- *перечень КИР, на основании которых определяется значение показателя;* (прим. переменные расчета)

- *пороговое значение, при превышении которого должны применяться меры, направленные на снижение Риска ИБ, с обоснованием их установления;* (прим. непосредственно значение показателя)

- *порядок реагирования на превышение пороговых значений, в том числе процедуры эскалации;*

- *периодичность расчета.* (прим. Периодичность нам задали жестко в ПУР)

Мониторинг Риска ИБ

*8.7. Субъект **может не устанавливать** указанные выше значения для тех показателей уровня Рисков ИБ, которые **не могут быть к нему применимы**. В этом случае Субъект **должен** иметь **документально** оформленное обоснование исключения такого показателя уровня Риска ИБ.*

*8.8. Участник **может** использовать **дополнительные показатели** уровня Рисков ИБ в дополнение к приведенным выше.*

*8.9. Мониторинг показателей уровня Риска ИБ **должен** осуществляться **на основании расчетных значений КИР**.*

*8.10. Субъекты **должны** определить **наборы КИР** согласно применимым к ним показателям уровня Риска ИБ.*

Мониторинг Риска ИБ

*8.11. Для каждого **КИР** должны быть установлены:*

- *количественное измерение КИР;*
- *способ расчета КИР;*
- *периодичность **пересмотра** КИР для поддержания КИР в актуальном состоянии;* (прим. срок в п.8.12 – раз в год)
- *периодичность **расчета** КИР;*
- ***состав информации**, используемой для расчета КИР, и ее источников, включая способ получения такой информации;*
- ***пороговые значения КИР** с обоснованием их установления;*
- ***работник**, ответственный за предоставление данных для расчета КИР и (или) расчет КИР;*
- ***порядок реагирования** на превышение пороговых значений КИР, в том числе процедуры эскалации.*

Мониторинг Риска ИБ

*8.12. **КИР и контрольные значения КИР** должны пересматриваться **не реже одного раза в год**.*

*8.13. Субъекты **должны** по **запросу** в установленным им сроки и порядке предоставлять Оператору сведения об установленных КИР, их контрольных значениях, установленных значениях показателей уровня Риска ИБ. Рекомендации по формированию и содержанию отчетности указаны в Приложении № 1 настоящего документа.*

Прил.1 Рекомендации к оформлению отчетной документации о показателях уровня Риска ИБ

В отчетную документацию рекомендуется включать следующую информацию:

- *описание каждого показателя уровня Риска ИБ;*
- *установленное контрольное значение для каждого показателя уровня Риска ИБ;*
- *значение каждого показателя уровня Риска ИБ за период;*
- *перечень КИР для каждого показателя уровня Риска ИБ. Для каждого КИР должно быть указано:*

- *описание КИР;* (прим. в п. 8.11 нет такого требования, только тут)
- *количественное измерение КИР;*
- *установленное пороговое значение каждого КИР.*

Мониторинг Риска ИБ

*8.14. Субъекты **должны** учитывать **рекомендации** Оператора по **корректировки** КИР и показателям уровня Риска ИБ.* (прим. Предположительно новые изменения по мере изменения внешних факторов)

*8.15. Участники **должны уведомлять** Оператора **о фактах превышения порогового значения** для показателей уровня Риска ИБ, перечисленных в п. 8.3. Участники должны производить **уведомление в течение 24 часов** с **момента выявления факта** превышения показателя уровня Риска ИБ. Уведомление выполняется путем создания заявки проекте «Программа безопасности» на Портале. К заявке должна быть приложена документация о показателях уровня Риска ИБ, пороговое значение которых было превышено. Документация **должна** содержать сведения пороговых значениях показателей уровня риска ИБ, сведения о зафиксированных значениях показателей уровня риска ИБ, результаты выполнения установленного порядка реагирования на превышение показателя уровня риска ИБ. Если у Участника отсутствует доступ к Порталу, то Участник должен уведомить АО «НСПК» по электронной почте, направив письмо с указанной информацией на адрес mirsecurity@nspk.ru.*

*8.16. **Свидетельством** превышения показателей уровня Риска ИБ может являться превышение пороговых значений уровня Неправомерных операций, зафиксированное в рамках процесса контроля уровня Неправомерных операций на стороне Участников, установленного документом [5]. **Обработка событий превышения** пороговых значений уровня **Неправомерных операций** осуществляется в соответствии с **положениями документа [5].***

[5] Стандарт ПС «Мир». Контроль уровня неправомерных операций на стороне Участников ПС «Мир»

Мониторинг Риска ИБ

Прил.1 Рекомендации к оформлению уведомления о фактах превышения порогового значения для показателей уровня Риска ИБ (прим. Прямой отсылки к порядку нет по тексту)

***В уведомление о фактах превышения** порогового значения для **показателей уровня Риска ИБ** рекомендуется включать следующую информацию:*

• *описание каждого показателя уровня Риска ИБ;*

• *установленное контрольное значение для каждого показателя уровня Риска ИБ;*

• *значение каждого показателя уровня Риска ИБ за период;*

• *перечень КИР для каждого показателя уровня Риска ИБ. Для каждого КИР должно быть указано:*

- *описание КИР;*
- *количественное измерение КИР;*
- *установленное пороговое значение каждого КИР.*

Совершенствование СУР ИБ

9. Совершенствование СУР ИБ Субъекта должно осуществляться в следующих случаях:

• *выявление* ***фактов или возможности превышения уровня Рисков ИБ*** *Субъекта;*

• *изменение* ***политики*** *Субъекта в отношении* ***принципов и приоритетов*** *в реализации СУР ИБ;*

• *изменение* ***политики*** *Субъекта в отношении* ***величины допустимого Риска*** *ИБ,* ***значений уровня Риска ИБ****;*
• ***внедрение новых технологий****, изменение информационной инфраструктуры Субъекта;*

• ***изменение условий взаимодействия*** *Субъекта с* ***третьими сторонами****, в том числе с другими Субъектами и платежными сервис-провайдерами;*

• *принятие решения о* ***необходимости совершенствования*** *СУР ИБ по итогам анализа результатов аудита СУР ИБ, анализа результатов оценки соответствия требованиям безопасности, проведенной согласно документа [2], реагирования на Инциденты ИБ и восстановлении после их реализации;* (прим. По результатам вн.аудита)

• ***изменение законодательства*** *Российской Федерации, в том числе нормативных актов Банка России.*

Права и обязанности

10.1. Субъект ***должен*** *назначить* ***сотрудника****, ответственного* ***за взаимодействие с Оператором*** *в рамках настоящего Стандарта ПС «Мир» и предоставление соответствующей информации о Рисках ИБ и ИБ. По запросу АО «НСПК»* ***Субъект в срок, установленный в запросе****, должен предоставить Оператору сведения о назначенном сотруднике, посредством направления письма Оператору на электронный адрес: mirsecurity@nspk.ru.*

10.2. ***По запросу*** *Субъект* ***должен*** *предоставить Оператору* ***информацию и/или документы*** *по функционированию системы управления Рисками ИБ в сроки и в порядке, установленные в таком запросе. Документы могут быть запрошены в электронном виде или на бумажном носителе в виде копии, заверенной подписью уполномоченного лица Субъекта.*

10.3. Оператор ***осуществляет контроль за эффективностью*** *системы управления Рисками ИБ Системы регулярной основе,* ***не реже одного раза в год****. Контроль осуществляется посредством выборочного запроса информации об эффективности СУР ИБ у Субъектов Системы.* ***Для проведения анализа Оператор вправе запрашивать у Субъекта информацию и/или документы*** *по функционированию системы управления Рисками Субъекта. Субъект обязуется предоставить запрашиваемые информацию и/или документы в порядке и сроки установленные в запросе Оператора.* (прим. Проведение внешнего аудита / проверки)

Рекламная пауза

Стоимость лицензий: **180 тыс руб**[1]
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*

Благодарим за внимание!

ООО «Технологии и бизнес»

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

Беляев Денис
Управляющий партнер
Тел/факс: +7 (495) 128 13 54
Email: belyaev.d@businesstech.store

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