ТАБ Технологии Автоматизация Бизнес

Обзор требований НСПК

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)

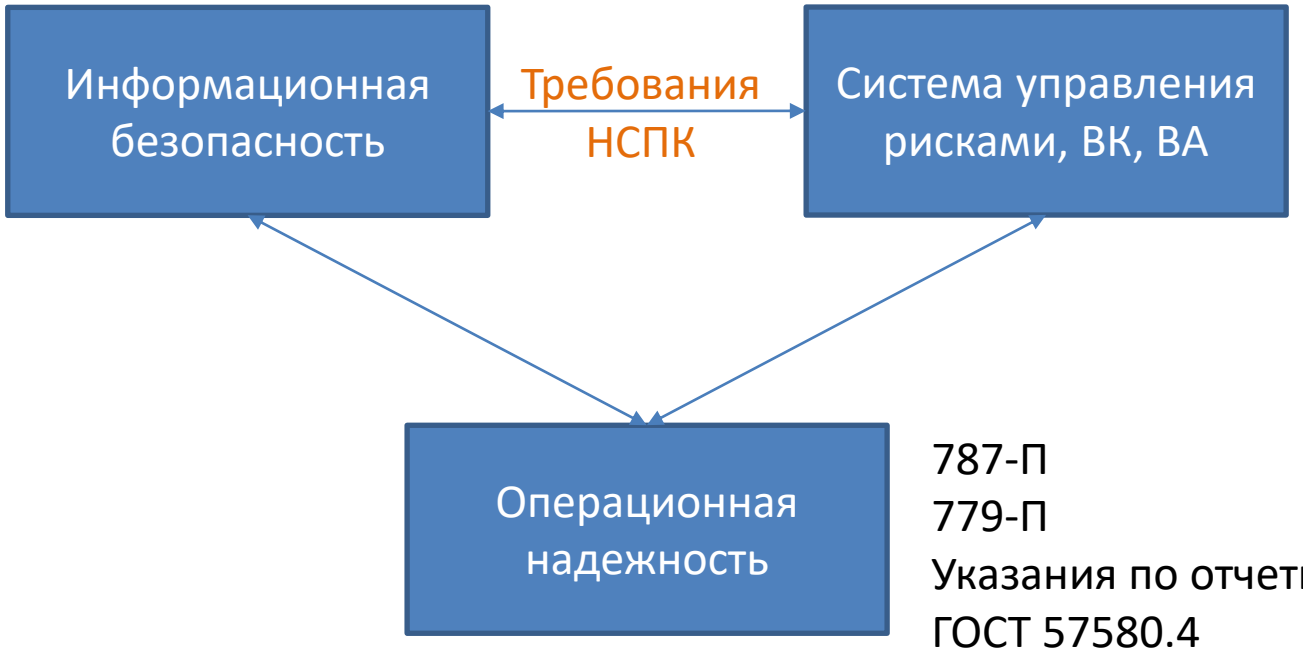
3. Базовая теория управления рисками

ТАБ Технологии Автоматизация Бизнес

Регуляторное окружение

Связь между внутренними процессами

683-П, 719-П,
802-П, 808-П
757-П
ГОСТ 57580.1
ГОСТ 57580.3



716-П,
4501-У, 5683-У
259-ФЗ
4015-ФЗ
и т.д.

787-П
779-П
Указания по отчетности
ГОСТ 57580.4

Это единые технические, методологические и организационные решения

716-П не противоречит требованиям НСПК и наоборот

Регуляторное окружение

ТАБ Технологии Автоматизация Бизнес

Кредитные организации

Опер. надежность

- 787-П

Информационная безопасность

- 683-П
- 719-П
- 802-П
- 808-П
- 821-П

Отчетность

- 6406-У

Некредитные финансовые организации

- 779-П
- ГОСТ 57580.3
- ГОСТ 57580.4

Применение не обязательно, до выпуска отдельного нормоакта

- ГОСТ 57580.1
- 757-П

- 6315-У, 6282-У, 6292-У, 6269-У, 6243-У

Отчетность действует по отраслям

Регуляторное окружение

Технологии Автоматизация Бизнес

	Кредитные организации	Некредитные финансовые организации	
Управление операционными рисками	744-П / 814-П	716-П	Частичное применение при вхождении в банковскую группу 814-П
		4501-У - ПУРЦБ	4060-У - НПФ
		4015-I ФЗ - ССД	Вн.ст. НАУФОР - УК
Внутренний контроль	242-П	402-ФЗ	
		5683-У - ПУРЦБ	Баз.ст. - НПФ
		4015-I ФЗ - ССД	УК нет

Регуляторное окружение

- Требования НСПК

Еще большая конкретизация подходов

- 716-П
- 787-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

Общие положения

1.1. Назначение и область применения документа

1.1.1. Настоящий Стандарт создан с целью обеспечения ***защиты информации при осуществлении переводов денежных средств*** *и* ***управления риском информационной безопасности[1] в Системе****.* (прим. национальная платежная система)

1.1.2. Настоящий Стандарт ПС «Мир» устанавливает основные требования к системе управления Рисками ИБ для ***Участников, ОПКЦ и РЦ*** *(кроме Банка России) (далее – Субъекты).*

1.1.3. Требования настоящего Стандарта распространяются на всех Субъектов.

1.2. Термины, определения и сокращения …
1.3. Нормативные ссылки …
1.4. Уведомления …

[1] Далее в документе под «Риском ИБ» будет пониматься риск ИБ, относящийся к указанной области действия

Основные положения

2.1. Субъект должен ***иметь функционирующую систему управления Риском ИБ****.*

2.2. Субъект должен управлять Риском ИБ ***в отношении платежных услуг, операционных услуг, услуг платежного клиринга и расчетных услуг в рамках ПС «Мир»****.*

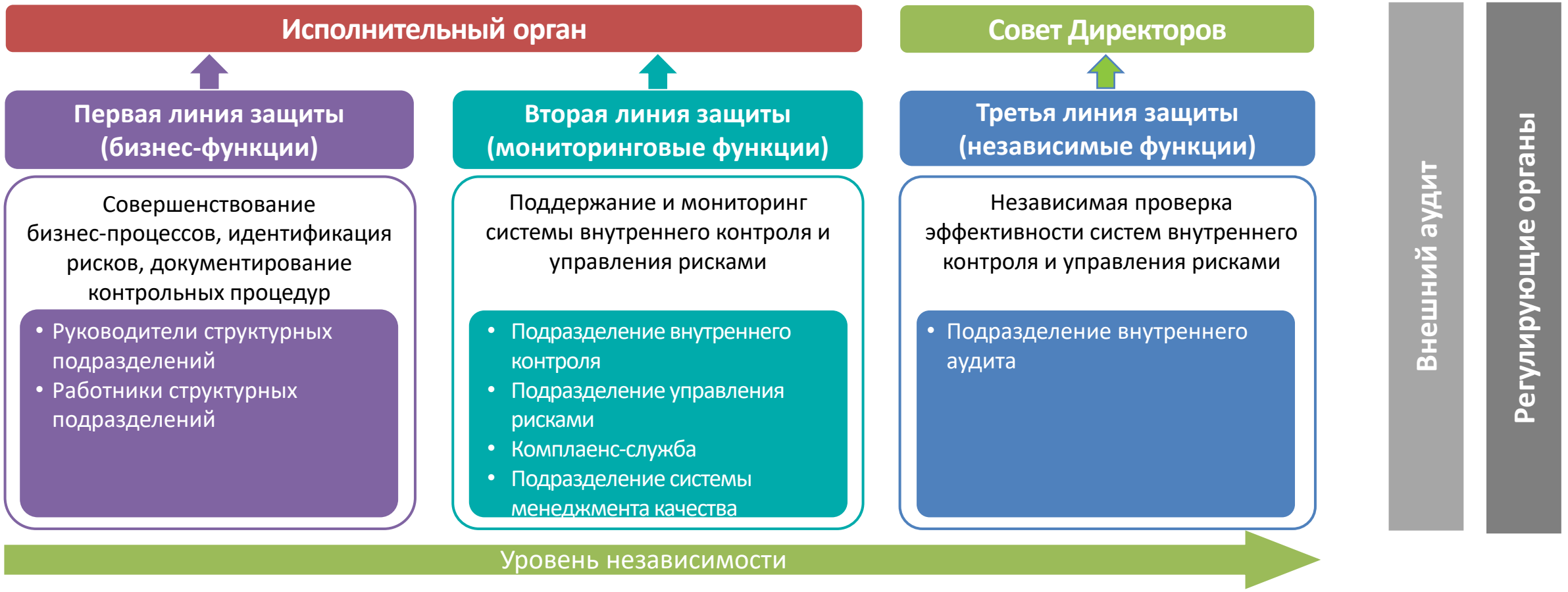
2.3. Система управления Риском ИБ Субъекта должна отвечать следующим требованиям:

• *Риск ИБ должен входить в состав* ***операционного*** *риска Субъекта*; (прим. отсылка к 716-П п.1.4. *Кредитная организация (головная кредитная организация банковской группы) для целей унификации управления операционным риском выделяет следующие виды операционного риска….:*

- *риск реализации угроз безопасности информации, которые обусловлены недостатками процессов обеспечения информационной безопасности*
- *операционный риск платежной системы)*

• *у Субъекта должна быть определена* ***организационная структура по управлению Риском ИБ****;*
(прим.
1-я линия – служба ИБ,
2-я линия – служба операционных рисков,
3-я линия – служба внутреннего аудита)

Концепция трех линий защиты



ГОСТ 57580.3 «Управление риском реализации информационных угроз» Введение
Следование принципу обеспечения «трех линий защиты», предполагающему выполнение действий в рамках непосредственного управления риском реализации информационных угроз «первой линией защиты», определение методологии, а также ее валидацию «второй линией защиты» и независимую оценку «третьей линией защиты»

Основные положения

• *процесс управления Риском ИБ должен быть* ***формализован****. Должны быть разработаны и утверждены нормативные документы, описывающие порядок управления Риском ИБ с учетом требований настоящего Стандарта* (прим. утверждает исполнительный орган или уполномоченный ими орган);

• *должна формироваться* ***регулярная отчетность об Инцидентах ИБ*** *и мерах реагирования, управления выявленными Инцидентами ИБ;* (прим. Требование 716-П
п.4.2. Подразделение, ***ответственное за организацию управления операционным риском****, формирует отчеты по операционному риску на ежеквартальной и ежегодной основе*
п. 4.2.4. ***Информация о событиях операционного риска****, включая* ***события риска информационной безопасности****, включается кредитной организацией (головной кредитной организацией банковской группы) в отчеты, указанные в подпункте 4.2.2 настоящего пункта, в разрезе направлений деятельности, в том числе в разрезе составляющих их процессов, типов событий операционного риска и источников операционного риска отдельно по видам операционного риска и содержит в том числе следующие показатели…*
В 716-П Нет прямого указания на меры реагирования и управления, в ГОСТ 57580.3 – есть, например п. 6.9)

• *система управления Рисками ИБ должна соответствовать* ***требованиям законодательства*** *Российской Федерации и требованиям нормативных актов Банка России.* (прим. отсылка к 716-П)

Организационная структура по управлению Риском ИБ

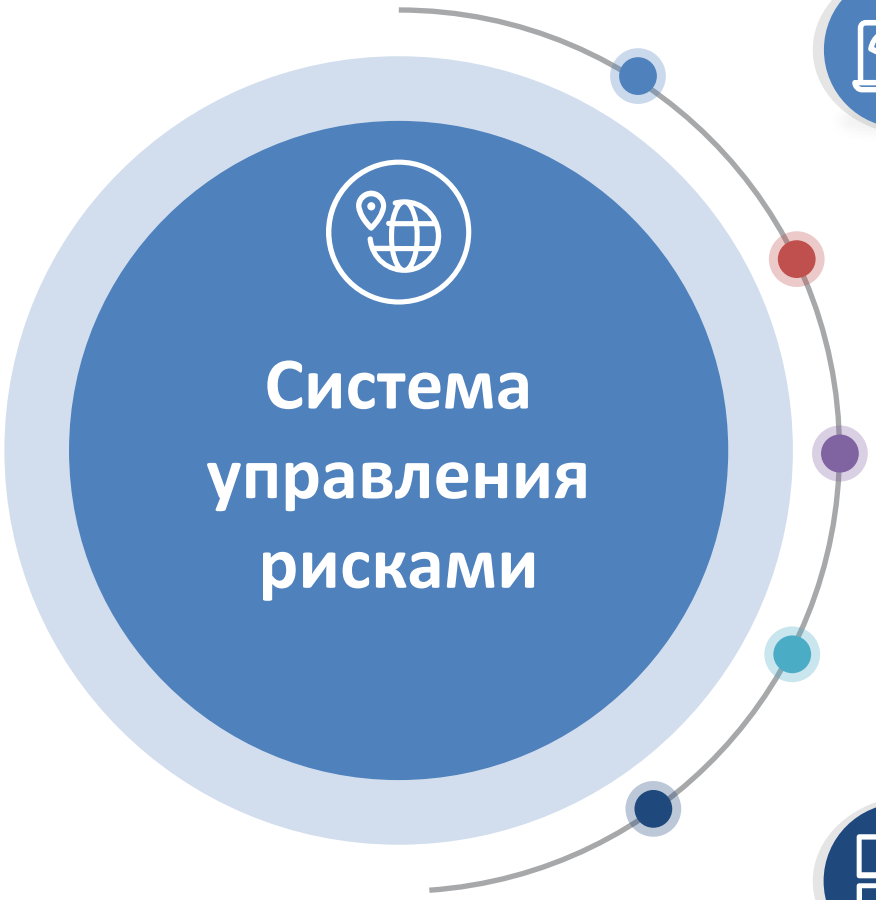
Технологии Автоматизация Бизнес

Субъекты **самостоятельно** определяют свою организационную структуру по управлению Риском ИБ в **соответствии с нормативными актами Банка России** или законодательством, применимым к Субъекту.

Выявление, идентификация, анализ и оценка Риска ИБ

ТАБ Технологии Автоматизация Бизнес

Внутренний аудит



01

Идентификация риска

Сбор информации о рисках и взаимосвязях, факторах и влиянии рисков; документирование в соответствии с принятой методологией; назначение ответственных.

02

Ведение основных данных

Определение организационной структуры; ведение матрицы рисков и сопутствующих справочников, классификатора рисков и категорий; подготовка опросных листов по рискам.

03

Анализ рисков

Проведение регулярной оценки и определение уровня рисков (включая получение информации от ответственных по риску и мероприятиям, в том числе с помощью опросов); различные шкалы оценки.

04

Реагирование

Документирование мероприятий для управление рисков, привязка к Процедурам контроля; управление статусом выполнения мероприятий и их эффективностью.

05

Мониторинг

Регистрация реализовавшихся рисков и потерь; непрерывный мониторинг показателей (КПУР, ПУР, КИР); формирование отчетности и дашбордов по рискам в различных разрезах.

Выявление, идентификация, анализ и оценка Риска ИБ

Инцидент	Риски	Анализ и оценка	Мониторинг (гл.8)
DDOS-атака	Поймаем вирус Взломают платежную систему и отправят средства Взломают критичного поставщика Утечка данных	Чем вызвана DDOS-атака? К чему может привести? Какой убыток мы понесем?	Если DDOS-атака больше 1 Тбит/с, нужно расширить подписку cloudflare
Выявление - Определение, что риск присущ	**Идентификация** - добавление в список риска	**Анализ и оценка** – Определение причин и последствий (качественно и/или количественно)	**Мониторинг** – Определение КИР и при его нарушении принятие мер

Выявление, идентификация, анализ и оценка Риска ИБ

Технологии Автоматизация Бизнес

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

Выявление, идентификация, анализ и оценка Риска ИБ

4.1 Субъект должен выявлять и идентифицировать Риски ИБ.

4.2 Процессы выявления и идентификации Рисков ИБ должны быть направлены на ***идентификацию событий, действий, условий****, которые могут оказать* ***влияние*** *на информационные системы и бизнес-процессы, реализующие платежные услуги, операционные услуги, услуги платежного клиринга и/или расчетные услуги в рамках ПС «Мир», а также* ***определение возможных последствий, анализ причин и источников возникновения*** *событий Рисков ИБ.*

(прим. опять ограничение по процессу, но 716-П требует идентифицировать все виды операционных рисков *716-П п.2.1.1. Идентификация операционного риска, включающая следующие способы*)

Выявление, идентификация, анализ и оценка Риска ИБ

4.3 Выявление и идентификация Риска ИБ должны включать следующие способы, но не ограничиваясь:

• *анализ произошедших Риск-событий; (*прим. *716-П п.2.1.1 аб.2 анализ базы событий;)*

*(*прим. пропущен способ с 716-П – самооценка путем анкетирования*)*

• *анализ динамики количественных показателей, направленных на измерение и контроль уровня Риска ИБ в определенный момент времени (показателей уровня Риска ИБ, ключевых индикаторов риска), по направлениям деятельности, в том числе в разрезе составляющих их процессов, Субъекта в соответствии с разделом 8 настоящего документа; (*прим. 716-П п.2.1.1 аб.4 дословно до слова Субъекта*)*

• *интервью с работниками Субъекта, в рамках которых работниками и руководством Субъекта обсуждаются Риски ИБ, оказывающие влияние на Систему; (*прим. 716-П п.2.1.1 аб.5 до 2го слова Субъекта, далее уточнение процесса. Пропущен аб.6 про предписания регуляторов*)*

• *анализ информации уполномоченного подразделения и внешнего аудита; (*прим. 716-П п.2.1.1 аб.7 дословно*)*

• *анализ информации работников Субъекта, полученной в рамках инициативного информирования работниками Субъекта службы управления рисками и (или) службы внутреннего аудита; (*прим. 716-П п.2.1.1 аб.8 дословно. Пропущен аб.9 по инициативному информированию*)*

• *анализ других внешних и внутренних источников информации и способов выявления Рисков ИБ. (*прим. 716-П п.2.1.1 аб.10*)*

Идентификация

Технологии Автоматизация Бизнес

Источники идентификации	Реестр рисков	Реестр значимых рисков
Риск-сессия Обмен опытом (семинары, новости и тд) Инциденты	Поймаем вирус Взломают платежную систему и отправят средства Взломают критичного поставщика Утечка данных DDoS-Атака Фишинговая атака	Поймаем вирус Утечка данных Фишинговая атака

Это процессы выявления рисков

- Если присущий риск > допустимый, то это значимый риск.
- Уровень допустимости в идеале СД, но может СУОР
- Работаем далее только со значимыми
- Если инцидент, по незначимому, то покрывается резервом по опер. риску

Выявление, идентификация, анализ и оценка Риска ИБ

Технологии Автоматизация Бизнес

4.4 Субъект должен использовать ***результаты процедуры выявления и идентификации*** *Рисков ИБ для* ***проведения процедур оценки Рисков ИБ*** *и корректного* ***учета связи*** *идентифицированного Риска ИБ с* ***произошедшими Риск-событиями****.* (прим. такой связи явно не указано в 716-П, но это общая практика)

4.5 Субъекты ***самостоятельно*** *определяют* ***методику*** *оценки Рисков ИБ, которая должна включать:*

- *шкалу оценки воздействия Риска ИБ*[2]*;*
- *шкалу вероятности реализации Риска ИБ;*
- *матрицу принятия решений по управлению Риском ИБ.*

4.6 Субъекты ***вправе*** *использовать количественные или качественные методы оценки Рисков ИБ.*
(Прим. явно определены шкалы для группы последствий)

[2] *В Приложении № 2 к настоящему документу приведена шкала оценки воздействия Рисков ИБ в Системе. Шкала оценки вероятности реализации риска и тепловая карта оценки риска приведены в Разделе 18 Правил ПС «Мир».*

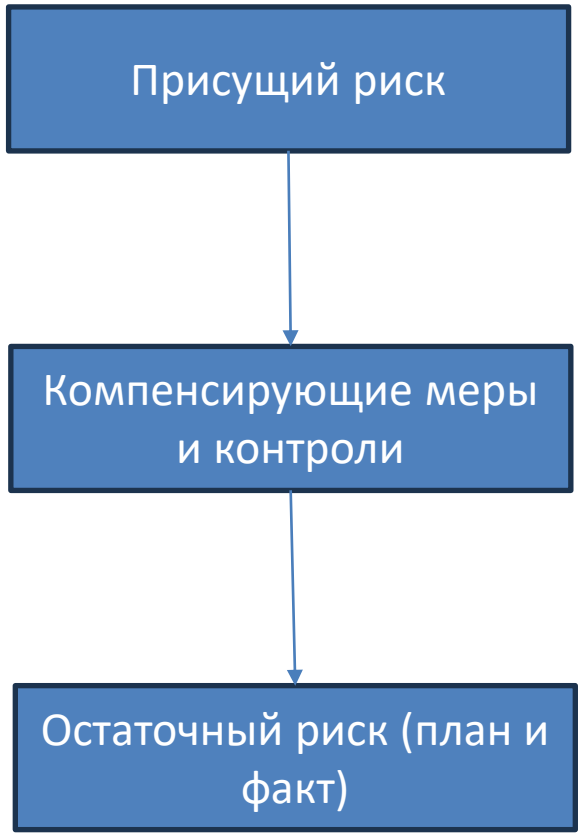
Рекламная пауза

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*

Порядок оценки риска



Присущий риск = Вероятность х Влияние

Меры применяем только к значимым рискам

Сумма снижения вероятности
Сумма снижения влияния

Остаточный риск (план) =
(Вероятность – Сумма снижение вероятности)
х (Влияние – Сумма Снижение влияния)

Факт – это фактическая оценка полученного эффекта

Методика может быть разная согласно п.4.5. Методика не определена ни в одном из нормоактов.

Порядок оценки риска

Технологии Автоматизация Бизнес

Риск: Фишинговая атака

- Шкала оценки вероятности реализации риска:

Вероятность	1 - крайне маловероятно	2 - маловероятно	3 - возможно	4 - очень вероятно	5 - почти точно
Частота реализации риска	реже, чем один раз в 5 лет	один раз в 3-5 лет	один раз в 1-3 года	один раз в 3-11 месяцев	один раз в 1-2 месяца

X

Вид негативных последствий / Уровень воздействия / уровень критичности Инцидента	Любое событие ИБ, вызванное нарушением требований безопасности в контуре ОПКЦ в результате действий третьих лиц, которое привело к краже или компрометации любых материалов или записей, содержащих данные платежных карт	Несанкционированный перевод денежных средств, инициированный операционным или клиринговым центром в результате нарушения требований безопасности в контуре ОПКЦ третьими лицами	Несанкционированный доступ к данным платежных карт в контуре Участника	Несанкционированный перевод денежных средств в контуре Участника
5 - очень сильное воздействие / максимальный уровень критичности	2 инцидента ИБ, которые произошли в течение 3 месяцев	От 2 млн руб.	Данные более 100 000 карт	Более 30 млн руб.
4 - сильное воздействие / высокий уровень критичности	2 инцидента ИБ, которые произошли в течение 6 месяцев	От 1 млн руб. до 1 999 999 руб.	Данные от 10 000 до 99 999 карт	От 10 000 000 до 29 999 999 руб.
3 - среднее воздействие / средний уровень критичности	1 инцидент ИБ в течение календарного года	От 0,01 руб. до 999 999 руб.	Данные от 500 до 9 999 карт	От 1 000 000 до 9 999 999 руб.
2 - низкое воздействие / низкий уровень критичности	–	–	Данные от 10 до 499 карт	От 500 000 до 999 999 руб.
1 - незначительное воздействие / низкий уровень критичности	–	–	Данные не более 10 карт	До 499 999 руб.

присущий риск: 5x2 = 10

Порядок оценки риска

Технологии Автоматизация Бизнес

Риск: Фишинговая атака

i	Компенсирующие меры и контроли	Бюджет	Вероятность	Влияние
1	Обучение персонала по работе с внешними электронными письмами	500 тыс. руб	-2	-0
2	Проведение периодического тестирования пользователей	1440 тыс руб/год	-0,5	-0
3	Закупка антивируса касперского для файловых серверов	200 тыс руб/ год.	-1	-0
	ИТОГО Воздействие мер и контролей:		**-3,5**	**-0**

Риск: Фишинговая атака

Присущий риск: 2х5= 10

Остаточный риск (план): 5(-3,5)х2(-0)=1,5х2= 3

Остаточный риск (факт) – определяем по переоценке риска, в следующий цикл
также определяет внутренний или внешний аудитор
также определяет управляющий по степени достижения КПЭ
контролируется через КИР

Если остаточный риск > допустимого, то нужно разработать дополнительные меры

Особенности

Вопрос: у нас в политике 716-П – матрица 3х3, а тут требуется 5х5. Нужно менять всю методологию и переоценивать другие оперриски не связанные с платежной системой?

Ответ: Нет, пересчитывать другие риски не обязательно. Методология управления рисками может содержать возможность добавления матриц к конкретному последствию или группе последствий (например объединенным присущим процессом). При этом, проще применять одну матрицу для всех последствий.

Последствие: остановка оказания услуг

Матрица 3х3

Последствие: несанкционированный доступ к данным платежным карт

Матрица 5х5

Выявление, идентификация, анализ и оценка Риска ИБ

4.7 Для анализа и оценки Рисков ИБ Субъект должен:

• *проводить **анализ и оценку внешних и внутренних факторов**, влияющих на информационную безопасность информационных систем и бизнес-процессов, реализующих платежные услуги, операционные услуги, услуги платежного клиринга и/или расчетные услуги в рамках ПС «Мир»;* (прим. Факторы – это источники и последствия рисков)
• *разработать и **поддерживать** в актуальном состоянии **классификаторы Рисков ИБ, Риск-событий, причин возникновения Риск-событий**;*
• *при **формировании перечня возможных Риск-событий** для каждого из бизнес-процессов учитывать **результаты моделирования угроз** информационной безопасности, результаты последней проведенной **оценки соответствия требованиям безопасности** (в соответствии с требованиями документа [2]), **наличия известных уязвимостей** в программном обеспечении, используемом для автоматизации оцениваемых бизнес-процессов;* (прим. Перечень возможных событий – это матрица рисков или иначе реестр рисков. Тут анализ - заполнение карточки риска.)
• *определить **уровни присущего Риска** ИБ для каждого из идентифицированных Рисков ИБ и **установить уровень допустимого** Риска ИБ;*
• *для выделения значимых для Субъекта Рисков ИБ сопоставить определенный уровень **присущего риска с установленным уровнем допустимого Риска ИБ** по каждому из идентифицированных Рисков ИБ;*
• *для каждого из значимых для Субъекта Рисков ИБ применить **способы управления рисками** и определить уровень остаточного Риска ИБ;*
• *для каждого из значимых для Субъекта Рисков ИБ **сопоставить уровни остаточного риска и допустимого Риска ИБ** и принять решение о необходимости применения других способов управления Рисками ИБ Субъекта в дополнение к ранее примененным способам управления Рисками ИБ;* (прим. Обычно делается управляющими с использованием дашборда)
• ***вести мониторинг** Рисков ИБ, в том числе уровней остаточных Рисков ИБ, и контролировать их соответствие допустимым уровням Рисков ИБ;* (прим. – речь про мониторинг КИР)
• ***оценить меры реагирования** на выявленные Риски ИБ;* (прим. речь управленческую оценку 1я линия и про вн. аудит – 3я линия)
• *составлять и актуализировать по результатам оценки Рисков ИБ Субъекта **профиль каждого идентифицированного** Риска ИБ Субъекта (далее – профиль Рисков ИБ).*

Выявление, идентификация, анализ и оценка Риска ИБ

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

4.9 **Оценка** Рисков ИБ должна выполняться **не реже одного раза в год**. (прим. В целом это обычно не приемлемый срок, средний срок – раз в месяц).

Ссылка на следующий вебинар

Технологии
Автоматизация
Бизнес

9 июня в 9:00мск

Регистрация и анонс в телеграмм канале ТАБ для Кредитных организаций

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