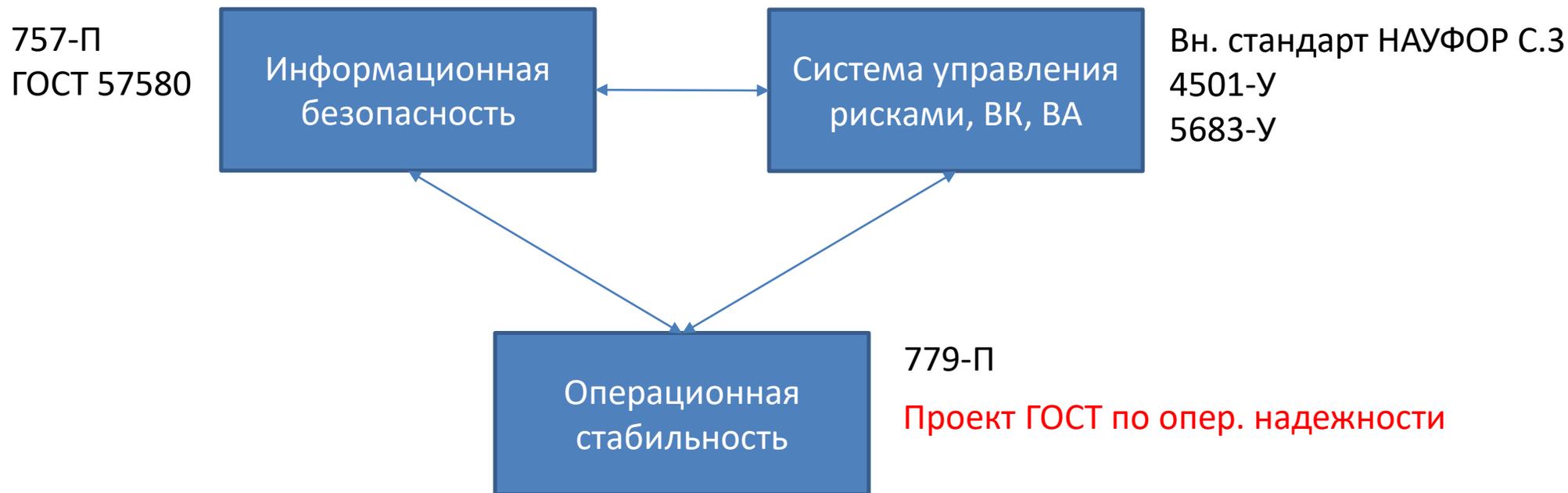


Практические особенности применения Положений Банка России №№ 779-П и 757-П

Презентационные материалы к семинару



Это единые технические, методологические и организационные решения

**ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ**



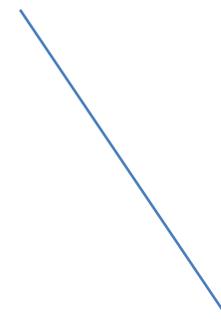
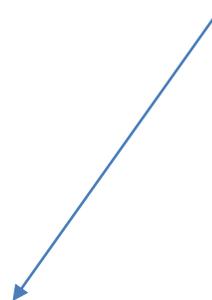
**НАЦИОНАЛЬНЫЙ
СТАНДАРТ
РОССИЙСКОЙ
ФЕДЕРАЦИИ**

ГОСТ Р
(проект)

**Безопасность финансовых (банковских) операций
ОБЕСПЕЧЕНИЕ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ
Базовый состав организационных и технических мер**

ГОСТ (проект)

**Безопасность финансовых (банковских) операций
ОБЕСПЕЧЕНИЕ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ
Базовый состав организационных и технических мер**



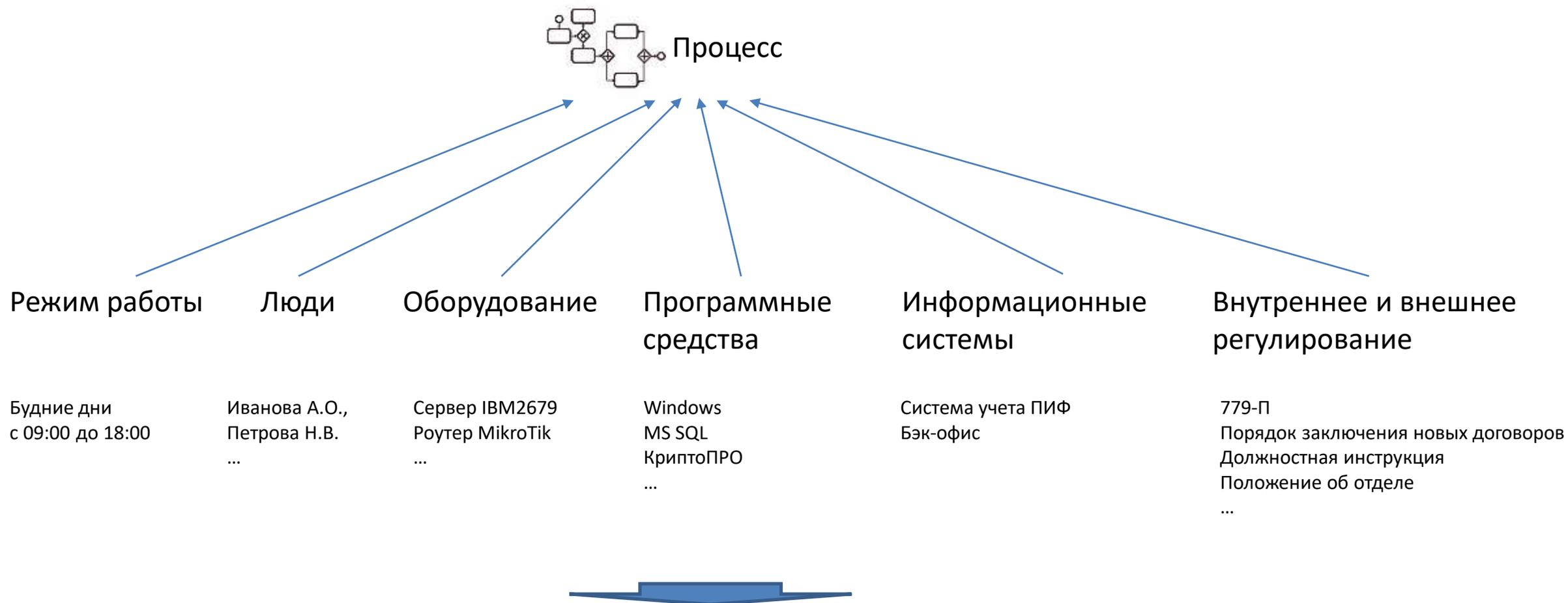
Уточнение формулировок:
Положения 779-П
Указание к 5709-У (отчетность)

Абсолютно новые требования

1 Практические особенности применения Положения Банка России № 779-П.

НФО должны обеспечивать организацию учета и контроля состава следующих элементов (при их наличии):

- **технологических процессов**, указанных в приложении к настоящему Положению, реализуемых непосредственно некредитной финансовой организацией;
- **подразделений (работников)** некредитной финансовой организации, ответственных за разработку технологических процессов, указанных в приложении к настоящему Положению, поддержание их выполнения, их реализацию;
- **объектов информационной инфраструктуры** некредитной финансовой организации, задействованных при выполнении каждого технологического процесса, указанного в приложении к настоящему Положению, реализуемого непосредственно некредитной финансовой организацией;
- **технологических участков** предусмотренных приложением к настоящему Положению технологических процессов, указанных в пункте 1.10 Положения Банка России от 20 апреля 2021 года № 757-П (далее - технологические участки технологических процессов), реализуемых непосредственно некредитной финансовой организацией;
- технологических **процессов**, указанных в приложении к настоящему Положению, технологических участков технологических процессов, **реализуемых внешними контрагентами**, оказывающими услуги в сфере информационных технологий, связанные с выполнением технологических процессов (далее - поставщики услуг);
- работников некредитной финансовой организации или иных лиц, осуществляющих физический и (или) логический доступ, или программных сервисов, осуществляющих логический доступ к объектам информационной инфраструктуры некредитной финансовой организации (далее - **субъекты доступа**), задействованных при выполнении каждого технологического процесса, указанного в приложении к настоящему Положению;
- взаимосвязей и взаимозависимостей между некредитной финансовой организацией и иными некредитными финансовыми организациями, кредитными организациями и **поставщиками услуг в рамках выполнения технологических процессов**, указанных в приложении к настоящему Положению (далее при совместном упоминании - участники технологического процесса);
- **каналов передачи защищаемой информации**, указанной в пункте 1.1 Положения Банка России от 20 апреля 2021 года № 757-П, обрабатываемой и передаваемой в рамках технологических процессов, указанных в приложении к настоящему Положению, участниками технологического процесса.



Надо определить (идентифицировать) свойства процесса, без которых он работать не сможет

Операционный риск

Более 20 тыс чистые потери
или
Уровень влияния Средний+



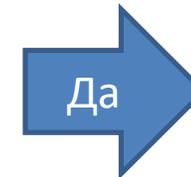
Причина риска информационная угроза?

И

Произошел во время режима работы?

И

Привел к неоказанию услуг?



Да

событие операционного риска,
связанное с нарушением
операционной надежности



Нет

событие операционного риска

- Допустимого отношения общего количества финансовых операций, совершенных во время деградации технологического процесса в рамках события операционного риска или серии связанных событий операционного риска, вызванных информационными угрозами, которые привели к неоказанию или ненадлежащему оказанию финансовых услуг (далее - события операционного риска, связанные с нарушением операционной надежности), к ожидаемому количеству финансовых операций за тот же период в случае непрерывного оказания финансовых услуг (далее - доля деградации технологических процессов);
- допустимого времени простоя и (или) деградации технологического процесса в рамках события операционного риска, связанного с нарушением операционной надежности (в случае превышения допустимой доли деградации технологического процесса), не выше порогового уровня, установленного в приложении к настоящему Положению;
- допустимого суммарного времени простоя и (или) деградации технологического процесса (в случае превышения допустимой доли деградации технологического процесса) в течение последних двенадцати календарных месяцев к первому числу каждого календарного месяца;



это КИРы

- показателя соблюдения режима работы (функционирования) технологического процесса (времени начала, времени окончания, продолжительности и последовательности процедур в рамках технологического процесса).



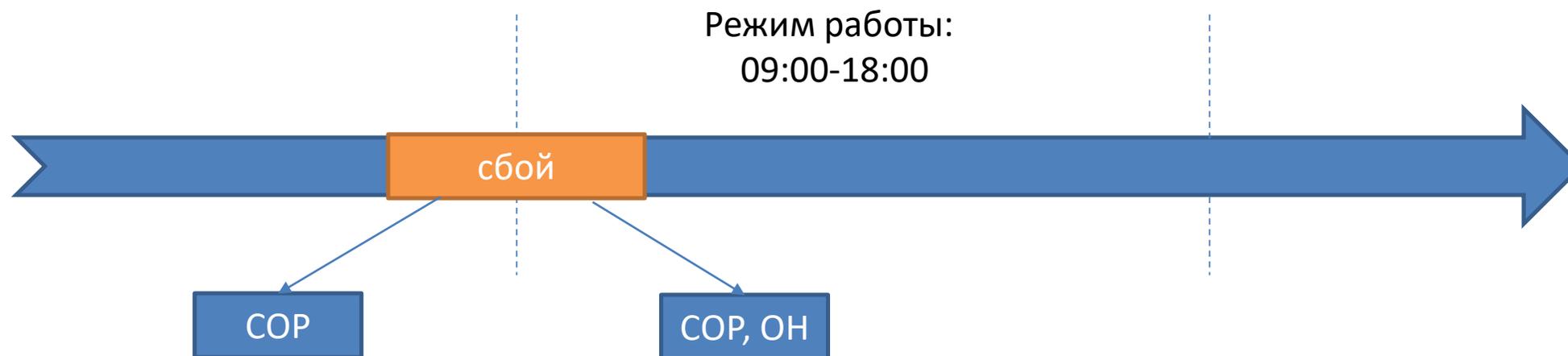
Это условие, является ли СОР инцидентом операционной надежности

«Допустимое время простоя и (или) деградации технологического процесса» указывается предельно допустимый для организации временной период, в течение которого происходит простой и (или) деградация технологического процесса, обеспечивающего деятельность в сфере финансовых рынков, в рамках события операционного риска или серии связанных событий операционного риска, вызванных информационными угрозами, которые привели к неоказанию или ненадлежащему оказанию финансовых услуг (далее – событие операционного риска, связанное с нарушением операционной надежности), в случае превышения допустимой доли деградации технологического процесса (информация по показателю указывается в минутах)

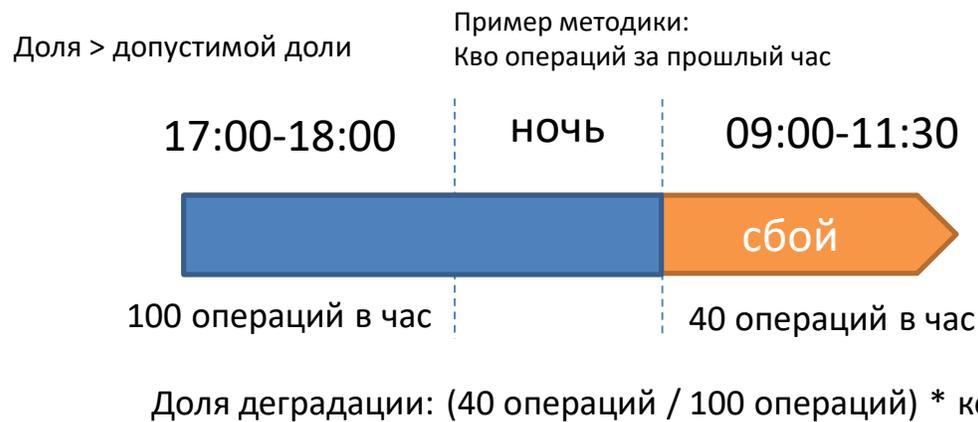
«Допустимая доля деградации технологического процесса» указывается допустимое отношение общего количества финансовых операций, совершенных во время деградации технологического процесса в рамках события операционного риска, связанного с нарушением операционной надежности, к ожидаемому количеству финансовых операций за тот же период в случае непрерывного оказания финансовых услуг (информация по показателю указывается в долях с точностью до шести знаков после запятой).

«Допустимое суммарное время простоя и (или) деградации технологического процесса» указывается предельно допустимое для организации суммарное время событий операционного риска, связанных с нарушением операционной надежности, в течение двенадцати календарных месяцев, исчисляемых с первого числа каждого календарного месяца, в течение которого происходят события операционного риска, связанные с нарушением операционной надежности, в случае превышения допустимой доли деградации технологического процесса (информация по показателю указывается в минутах)

«Суммарное время простоя и (или) деградации технологического процесса» указывается фактическое значение суммарного времени, в течение которого происходили события операционного риска, связанные с нарушением операционной надежности, за последние двенадцать календарных месяцев, в случае превышения допустимой доли деградации технологического процесса (информация по показателю указывается в минутах).



Расчет КИР: времени простоя/деградации и суммарного времени простоя/деградации



Посещаемость и график работы



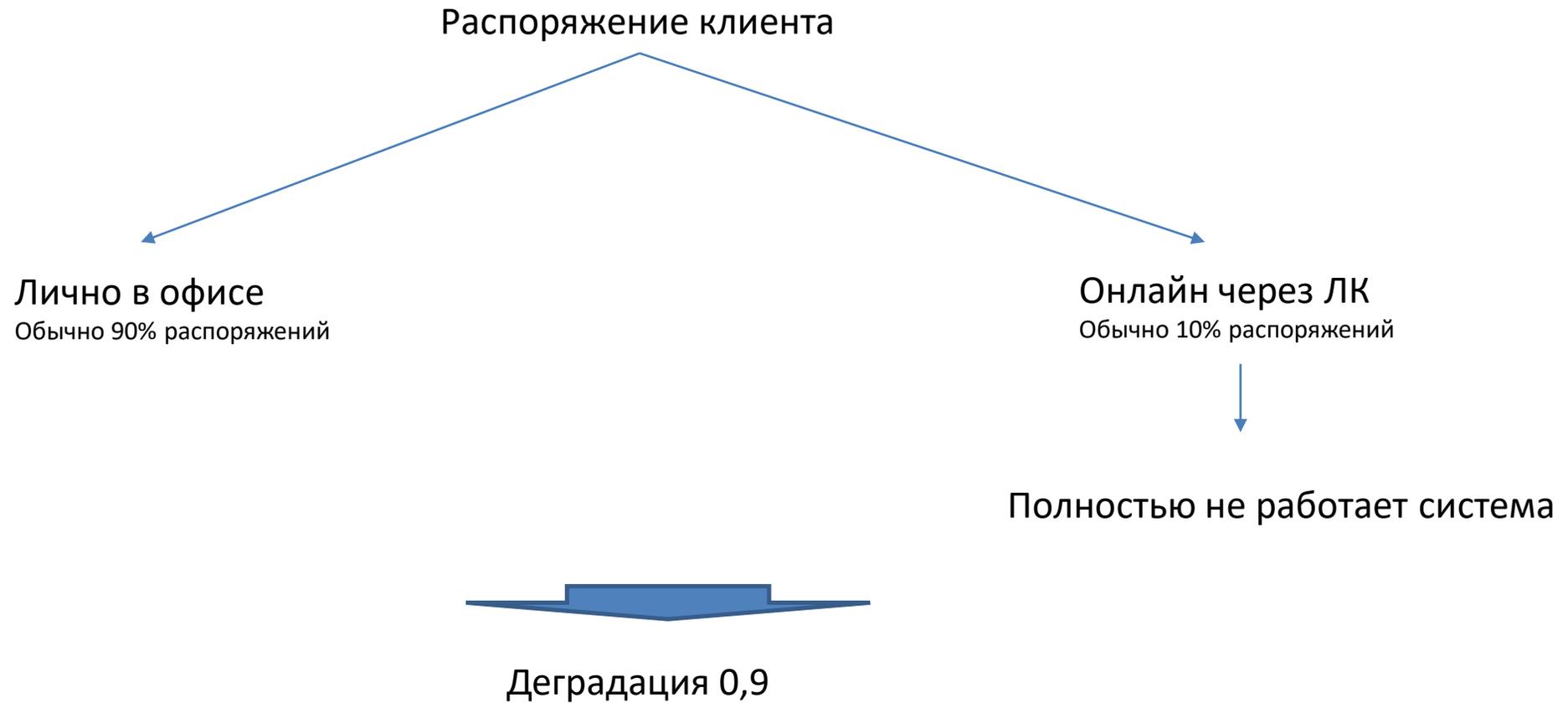
Проблематика:

- Как выявить само событие?
- Какие операции считать?
- Какая методика определения прошлого периода?
- Как собрать информацию об операциях?

Деградация из-за процессов



Деградация из-за онлайн/офлайн формата



Свод по рынку и варианты распределения

	Допустимая доля деградации	Допустимое время простоя	Допустимое суммарное время простоя
ЗПИФ недвижимости	1	1 440	100 000
ЗПИФ комбинированный БПИФ	1	тпрнфо26-27 1 440	100 000
		тпрнфо25 120 (реализация прав)	
ОПИФ	1	тпрнфо26-27 1 440	100 000
	0.9 - 0.99 (каналы сбыта)	тпрнфо25 120 (реализация прав)	
ДУ	1	тпрнфо6 240	100 000
	0.9 - 0.99 (каналы сбыта)	тпрнфо7 720	
		тпрнфо8 1 440	
Брокерская деятельность	1	тпрнфо1 120/240	100 000
	0.9 - 0.99 (каналы сбыта)	тпрнфо2 720	
		тпрнфо3 1 440	

2 Практические особенности применения Положения Банка России № 757-П.

Требования к информационной безопасности 757-П

Вступает в силу требования к применению ГОСТ 57580 к организациям с минимальным уровнем с 1 июля 2022 года

Таблица 1 Базовый состав мер по организации и контролю использования учетных записей субъектов логического доступа				
Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
УЗП.2	Контроль соответствия фактического состава разблокированных учетных записей фактическому составу легальных субъектов логического доступа	О	О	Т
УЗП.3	Контроль отсутствия незаблокированных учетных записей: - уволенных работников; - работников, отсутствующих на рабочем месте более 90 календарных дней; - работников внешних (подрядных) организаций, прекративших свою деятельность в организации	О	О	Т
УЗП.4	Контроль отсутствия незаблокированных учетных записей неопределенного целевого назначения	О	О	О
Таблица 2 Базовый состав мер по организации, контролю предоставления (отзыва) и блокированию логического доступа				
Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
УЗП.6	Назначение для всех ресурсов доступа распорядителя логического доступа (владельца ресурса доступа)	О	О	О
УЗП.7	Предоставление прав логического доступа по решению распорядителя логического доступа (владельца ресурса доступа)	О	О	О
УЗП.8	Хранение эталонной информации о предоставленных правах логического доступа и обеспечение целостности указанной информации	О	Т	Т
УЗП.9	Контроль соответствия фактических прав логического доступа эталонной информации о предоставленных правах логического доступа	О	Т	Т
УЗП.12	Контроль необходимости отзыва прав субъектов логического доступа при изменении их	О	О	О

Всего около 300
требований к
исполнению

Событие нарушения требования выполнения ГОСТ 57580 - это инцидент защиты информации, если он привел к потерям, то это рисковое событие операционного риска.

Влияет на отчетность по операционной стабильности 779-П, должно быть отражено в базе рисков.

О - организационно



В организации должен быть внутренний нормативный документ регулирующий исполнение организационно

Т - Технически



В организации должен быть программный продукт, реализующий требование технической мерой

УЗП.2

Контроль соответствия фактического состава разблокированных учетных записей фактическому составу легальных субъектов логического доступа

УЗП.3

Контроль отсутствия незаблокированных учетных записей:

- уволенных работников;
- работников, отсутствующих на рабочем месте более 90 календарных дней;
- работников внешних (подрядных) организаций, прекративших свою деятельность в организации

УЗП.23

Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала и пользователей, обладающих правами логического доступа, в том числе в АС, позволяющими осуществить операции (транзакции), приводящие к финансовым последствиям для финансовой организации, клиентов и контрагентов

УЗП.25

Регистрация событий защиты информации, связанных с действиями по управлению учетными записями и правами субъектов логического доступа

ПЗИ.5 Документарное определение порядка применения технических мер защиты информации, реализуемых в рамках процесса системы защиты информации, включающего:

- правила размещения технических мер защиты информации в информационной инфраструктуре;
- параметры настроек технических мер защиты информации и информационной инфраструктуры, предназначенных для размещения технических мер защиты информации <*>;
- руководства по применению технических мер защиты информации (включающие руководства по эксплуатации, контролю эксплуатации и использованию по назначению технических мер защиты информации);
- состав ролей и права субъектов доступа, необходимых для обеспечения применения технических мер защиты информации (включающего эксплуатацию, контроль эксплуатации и использование по назначению мер защиты информации)

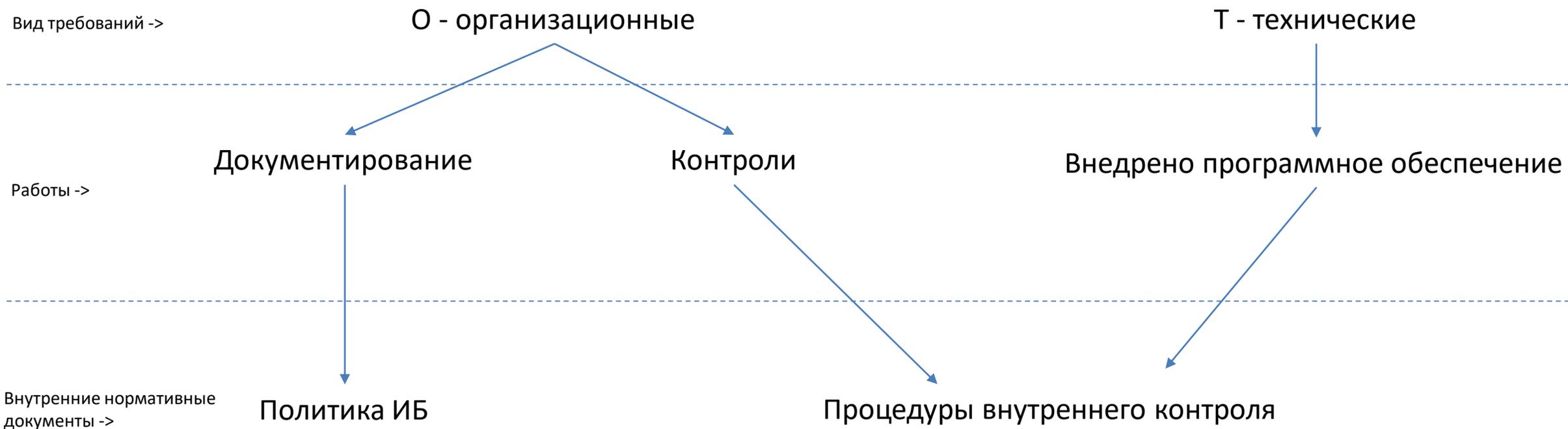
РЗИ.1

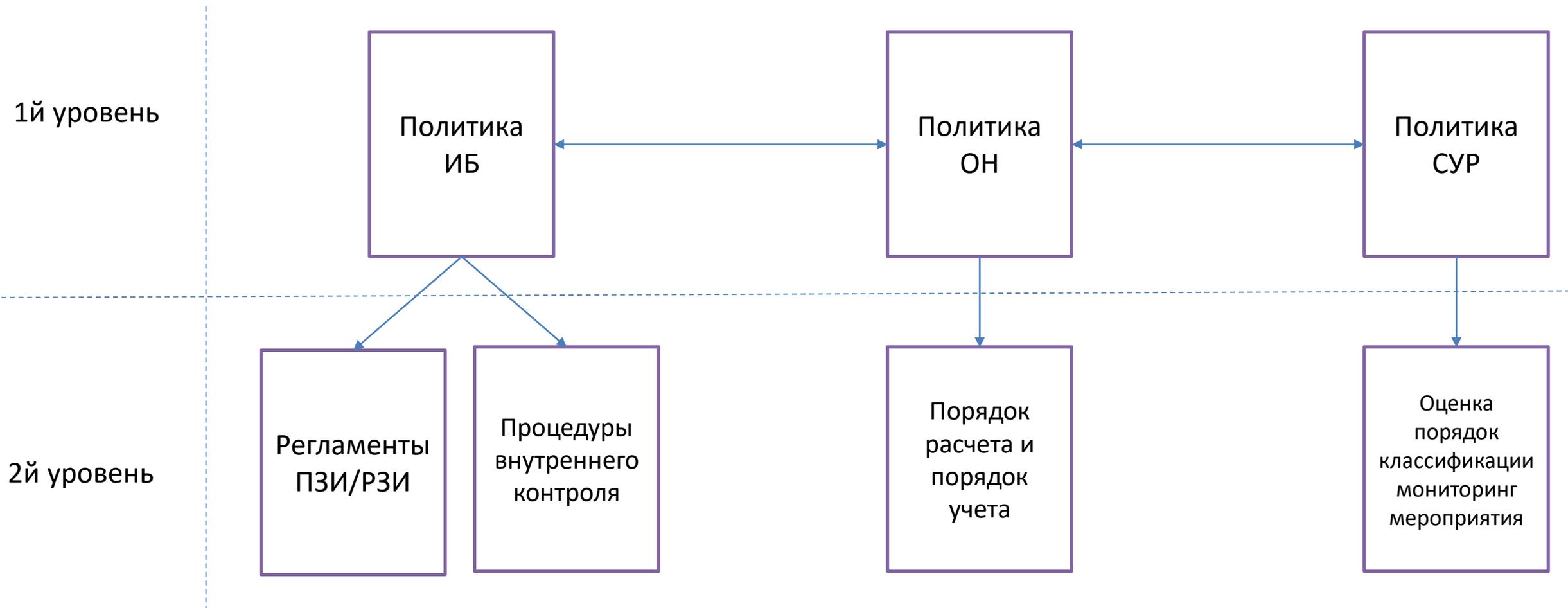
Реализация учета объектов и ресурсов доступа, входящих в область применения процесса системы защиты информации, для уровней информационной инфраструктуры, определенных в 6.2 настоящего стандарта

КЗИ.1

Контроль фактического состава объектов и ресурсов доступа, входящих в область применения процесса системы защиты информации, на соответствие учетным данным, формируемым в рамках выполнения меры РЗИ.1 таблицы 49

Предлагаемая схема ВНД





3 Практические особенности применения Положения Банка России № 779-П.

Основные ошибки при организации процессов ОН

Дубль учетных регистров и процессов организации.

Субъекты, ресурсы и объекты доступа дублируются у информационной безопасности и у риск-менеджеров

Нет учетных регистров субъектов, ресурсов и объектов доступа, в рамках требования РЗИ.1 ГОСТ 57580

ГОСТ 57580 предполагает частичное исполнение, но при этом учетные регистры являются базой для подавляющего большинства требований

Закупаются услуги по ГОСТ 27000, предполагая, что это решит вопросы по ГОСТ 57580

При этом поставщики выдают свои услуги по ГОСТ 27000, как решающие вопросы в том числе и ГОСТ 57580. ГОСТ 57580 и ГОСТ 27000 – это разные по содержанию документы. В итоге вы исполняете процессы, которые не требуются, при этом не исполняя те процессы, которые требуются. Лишние расходы при недостаточности решения

Детализация учета критичной архитектуры не достаточно

В среднем карточка ИС имеет от 20 до 50 учетных полей, в зависимости от объединения 779-П с ГОСТ 57580 или нет.

Детализация учета неверна

Например, организация вводит реестр технологических участков по некоторому своему пониманию, а это жестко заданный Банком России ограниченный не расширяемый список.

Неверный порядок трактовки ДДД (допустимой доли деградации)

Событие опер.риска – первично. Далее одно из критичных условий – должна быть ненадлежаще оказана услуга, например с жалобой. И только потом считается деградация и прочие целевые показатели.

Главный ответ, который получит организация при организации процессов СУОР и ОН:

Какие именно процессы не работают прямо сейчас или не работали в отчетном периоде

Дополнительная детализация:

1. Какое именно подразделение встало
2. Какой именно процесс встал
3. Какие чистые потери в рублях мы понесли
4. Какая динамика происходящих событий (увеличивается количество событий или уменьшается)
5. Нужно ли мне, как руководителю вовлекаться или пока простой находится в ожидаемой норме

Но! Формально это сейчас касается только риска информационной безопасности с влиянием на клиентов

Если процесс управления СОР и ОН организован, люди выделены, технические решения реализованы, события собираются и только потом отсеиваются ненужные ЦБ, почему бы их не использовать для управления?

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
+7 (926) 0261437

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

