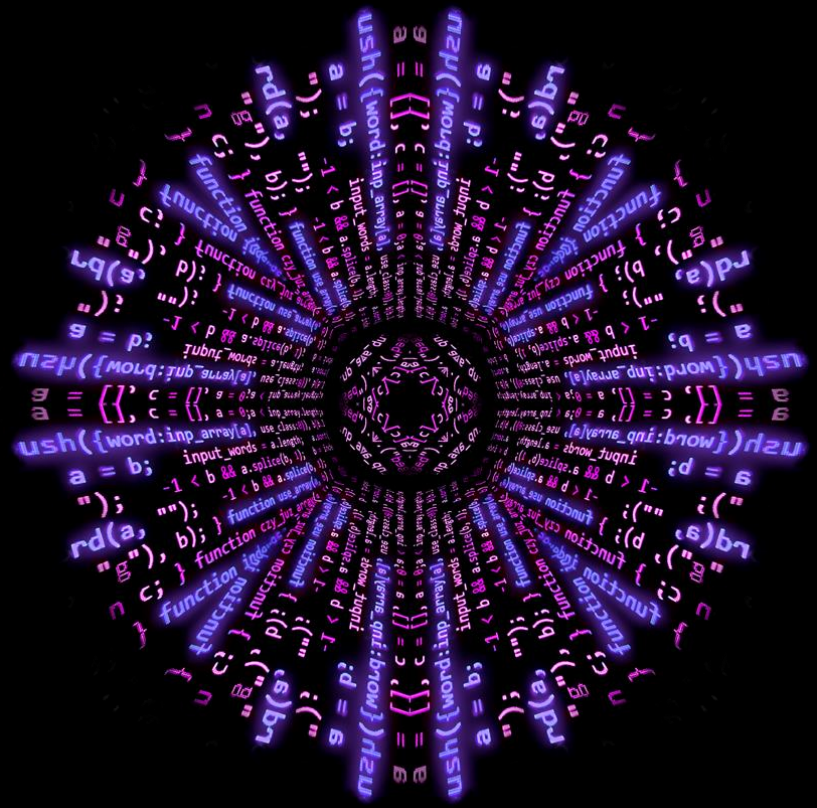
Deloitte.



Вебинар

Управление рисками информационных технологий

- Июнь 2020 года

MAKING AN IMPACT THAT MATTERS since 1845

Ведущие вебинара

Владимир Ремыга, CISA, CISSP, CGEIT, CRISK, PRINCE 2

Директор

vremyga@deloitte.com

+7 700 714 5505

Владимир руководит практикой консультационных услуг Deloitte в области ИТ рисков и кибер-безопастноси в Каспийском и Кавказском регионах. Обладая 25 летним опытом, он оказывает консультационные услуги для большого числа коммерческих и не коммерческих организаций и специализируется на услугах в направлении: цифровой трансформации, ИТ архитектуры, управления кибер-рисками, оптимизации ИТ затрат и повышения эффективности.

Ильяс Абельдинов, CISA

Менеджер

iabeldinov@deloitte.kz

+7 701 999 8008

Ильяс руководит проектами аудиторских и консультационных услуг Deloitte в области ИТ рисков и ИТ аудитов в Каспийском и Кавказском регионах. Он имеет более 10 лет опыта работы оказания аудиторских и консультационых услуг для крупных частных компаний, а также компаний государственного и квази-государственного сектора.

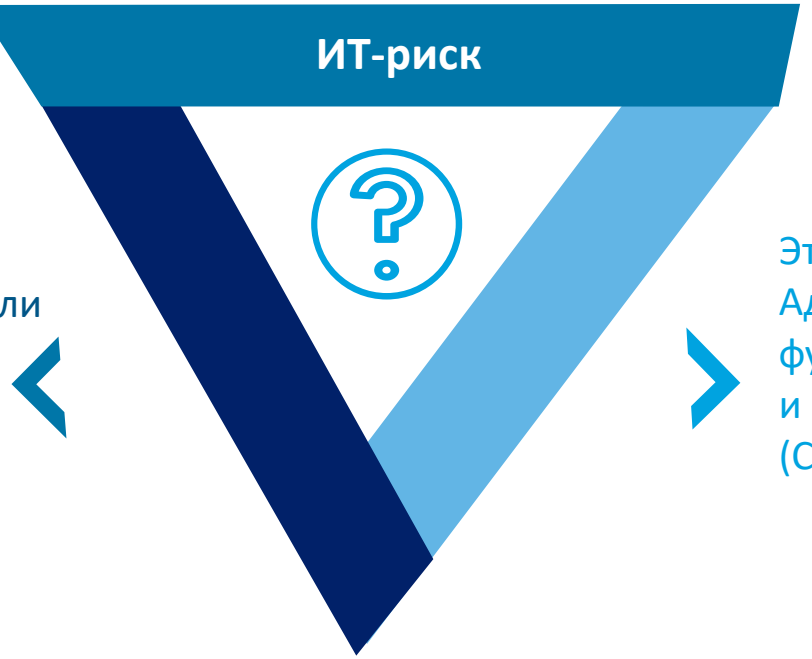
Регуляторные требования: Постановление Правления НБРК №188
Правила формирования системы управления рисками и внутреннего контроля для банков второго уровня

- В соответствии с ПП НБРК №188 от 12 ноября 2019 года, Правлением НБРК были утверждены Правила формирования системы управления рисками и внутреннего контроля для банков второго уровня.
- Банки второго уровня обязуются привести свою деятельность в соответствие с требованиями данного постановления в срок до 1 июля 2020 года.
- Глава 8 (управление рисками информационных технологий) данного постановления, описывает обязательные требования по управлению ИТ-рисками.

- Согласовании планов мероприятий по реализации стратегии банка в части обеспечения доступности информационно-коммуникационных технологий.
- Определение потребностей в ИТ-ресурсах для обеспечения непрерывности бизнес процессов.
- Примеры требуемых мероприятий в области информационно-коммуникационных технологий с указанием сроков и ответственных за их реализацию.

Что такое ИТ-риск

Информационные риски – это опасность возникновения убытков или ущерба в результате применения компанией информационных технологий.



Это бизнес риск, связанный с приобретением, Адаптацией, использованием, владением, функционированием
и эксплуатацией ИТ в компании
(Cobit 5 for Risk).

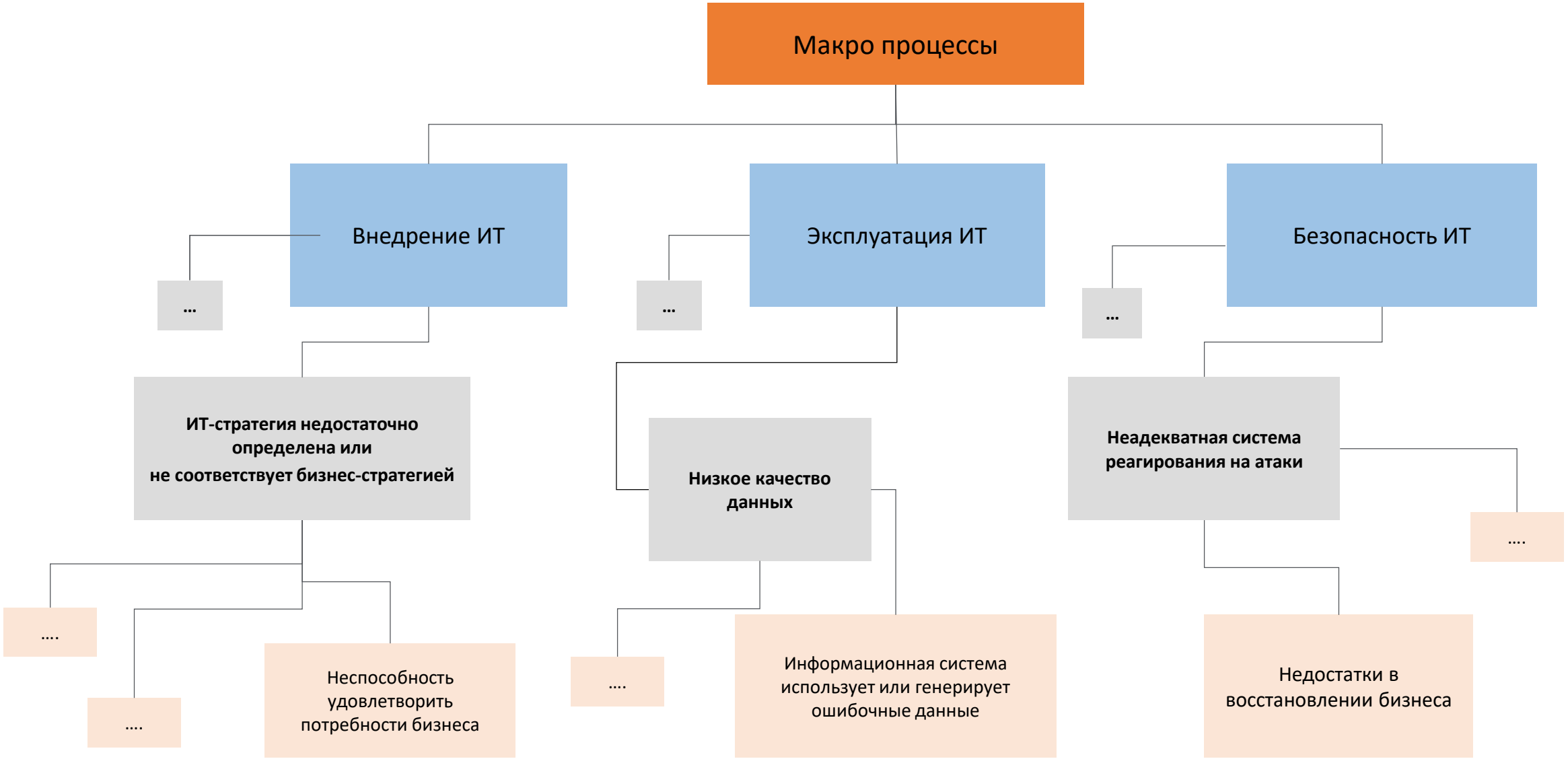
Матрица ИТ-рисков

Таблица 2 Матрица ИТ-рисков

№	Индентификатор риска	Описание риска
1.	IT-01	Заражение компьютерными вирусами
2.	IT-02	Использование нелицензионных программ
3.	IT-03	Неавторизованный доступ к информационным системам
4.	IT-04	Ошибка при техническом обслуживании серверного оборудования
5.	IT-05	Сбой в системе электропитания в серверной
6.	IT-06	Сбой систем кондиционирования серверов
7.	IT-07	Технический сбой серверного оборудования
8.	IT-08	Технический сбой сетевого оборудования
9.	IT-09	Кража, преднамеренная порча носителей данных (жестких дисков и иных носителей)
10.	IT-10	Неавторизованный доступ к носителям данных (жестким дискам и иным носителям)
11.	IT-11	Пожар в серверной комнате
12.	IT-12	Затопление серверной комнаты
13.	IT-13	Программный сбой в информационной системе
14.	IT-14	Требования заказчика разработки программного обеспечения не формализованы
15.	IT-15	Некорректное составление технического задания для кодировщиков программного обеспечения
16.	IT-16	Ошибка при написании кода программного обеспечения
17.	IT-17	Ошибка при внедрении разработанного программного обеспечения
18.	IT-18	Несвоевременное оказание услуг в рамках сопровождения автоматизированных рабочих мест клиентов
19.	IT-19	Несвоевременное размещение обновления автоматизированных рабочих мест клиентов на интернет-сайте
20.	IT-20	Несвоевременное уведомление ответственных лиц клиентов о необходимости обновления автоматизированного рабочего места

Пример

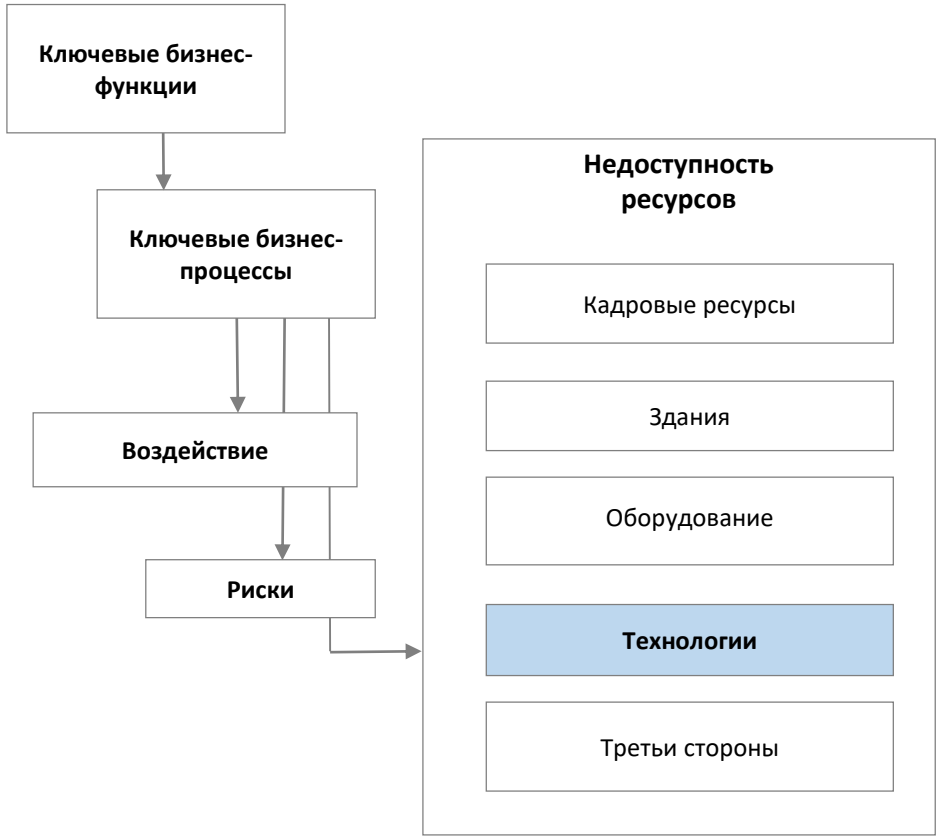
Факторы ИТ-рисков



Пример факторов риска

Процесс макро	Первичные факторы ИТ-риска	Вторичные факторы ИТ-риска
Внедрение ИТ	Недостаточное участие органа управления	• Недостаточное понимание проблем • Неправомерные решения • Недостаточный контроль
	ИТ-стратегия неадекватно определена или согласовано с бизнес-стратегией	• Неспособность предвидеть потребности бизнеса и технологические процессы: обновления / проблемы/использование • Неадекватные инструменты и уровень обслуживания
	Недостаточное управление бюджетом	• Недостаточное согласование бюджета со стратегией • Несуществующие или недостаточно четкие распределения бюджета • Ненадлежащий надзор за расходами
	Роли и обязанности ИТ и функции информационной безопасности	• Плохо определенные, распределенные или взаимодейственные роли и обязанности • Неадекватный или недостаточный штат сотрудников
	Неадекватная рационализация ИТ	• Отсутствие контроля над архитектурой информационных систем (урбанизация) • Несогласованные ИТ-стандарты • Неспособность справиться с устареванием оборудования
	Недостаточный контроль за аутсорсингом	• Неадекватная договорная база • Сверхзависимость • Неадекватный контроль за уровнем обслуживания • Неадекватная процедура обратимости
	Несоблюдение законодательных и нормативных требований	• Бизнес-потребности не соответствуют действующему законодательству • ИТ-разработки не соответствуют юридическим инструкциям бизнес-направлений • ИТ-стандарты не соответствуют действующему законодательству
	Неадекватное управление рисками	• Несуществующее или частичное отображение рисков • Неадекватная система управления • Неадекватное обнаружение и управление инцидентами операционного риска • Неадекватная система периодического контроля

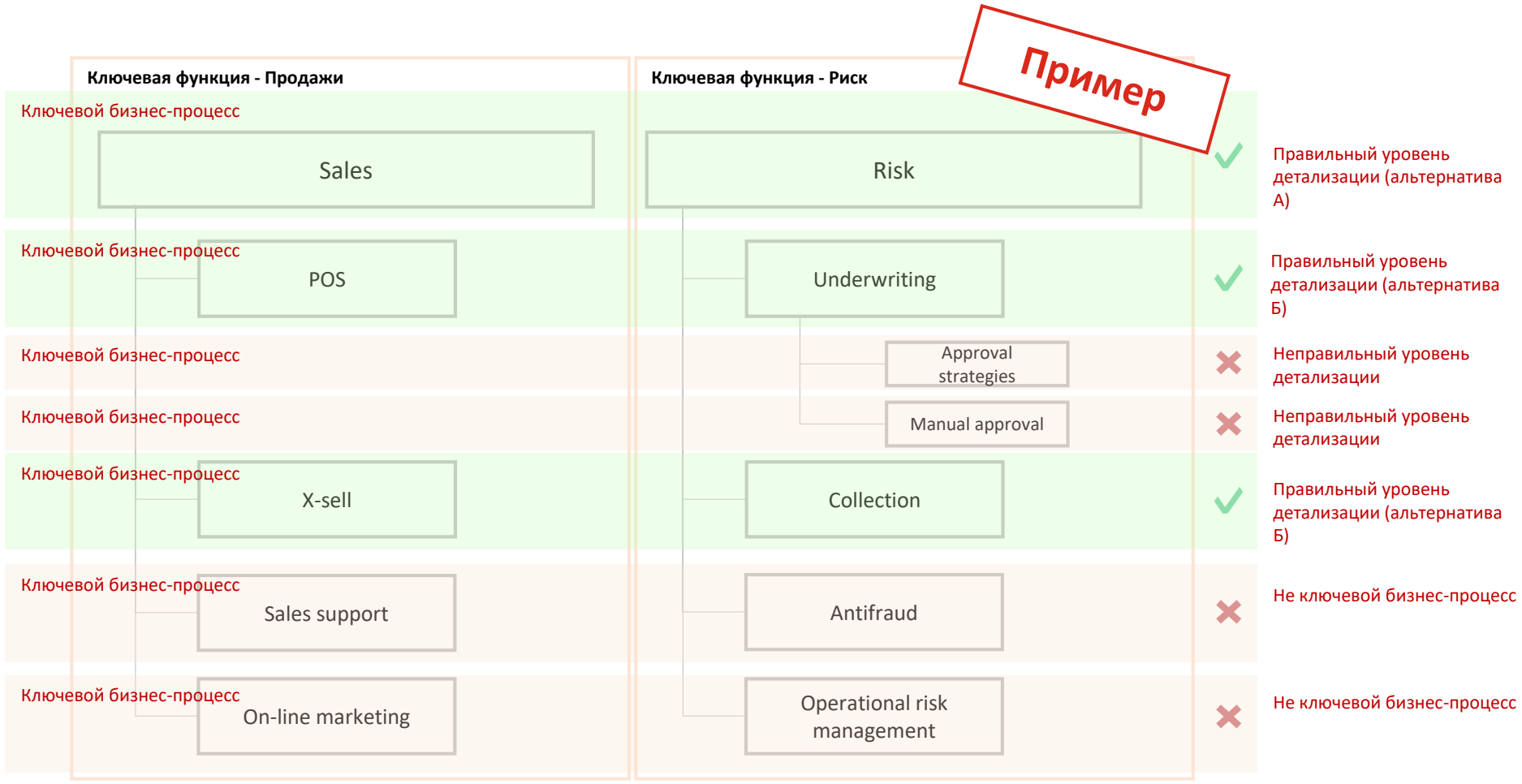
Анализ влияния на бизнес



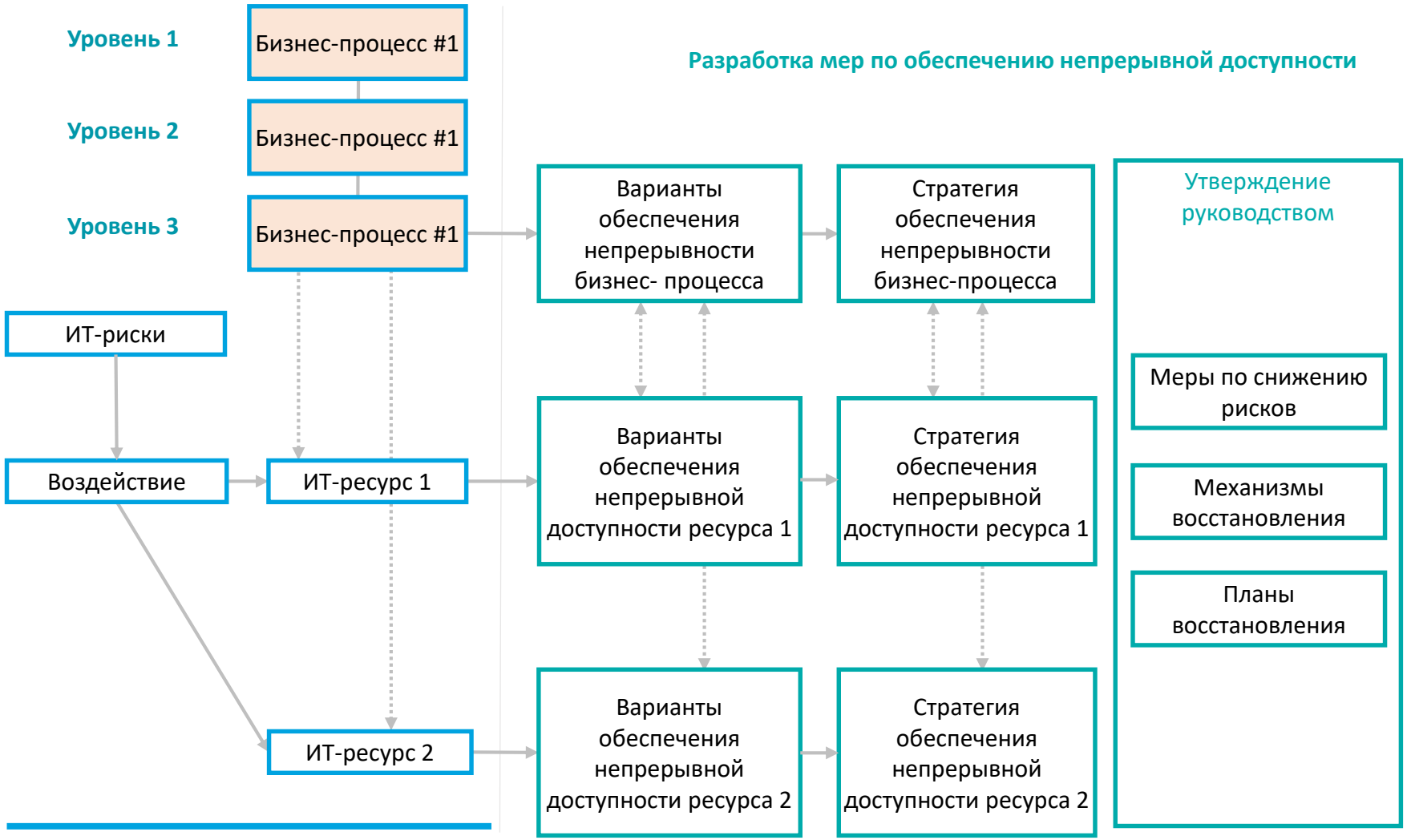
Что если?

- Вы не можете попасть в офис?
- Вы не можете нанять нового сотрудника?
- Вы не можете производить начисление зарплаты?
- Один из ваших лучших сотрудников ИТ подразделения уволился?

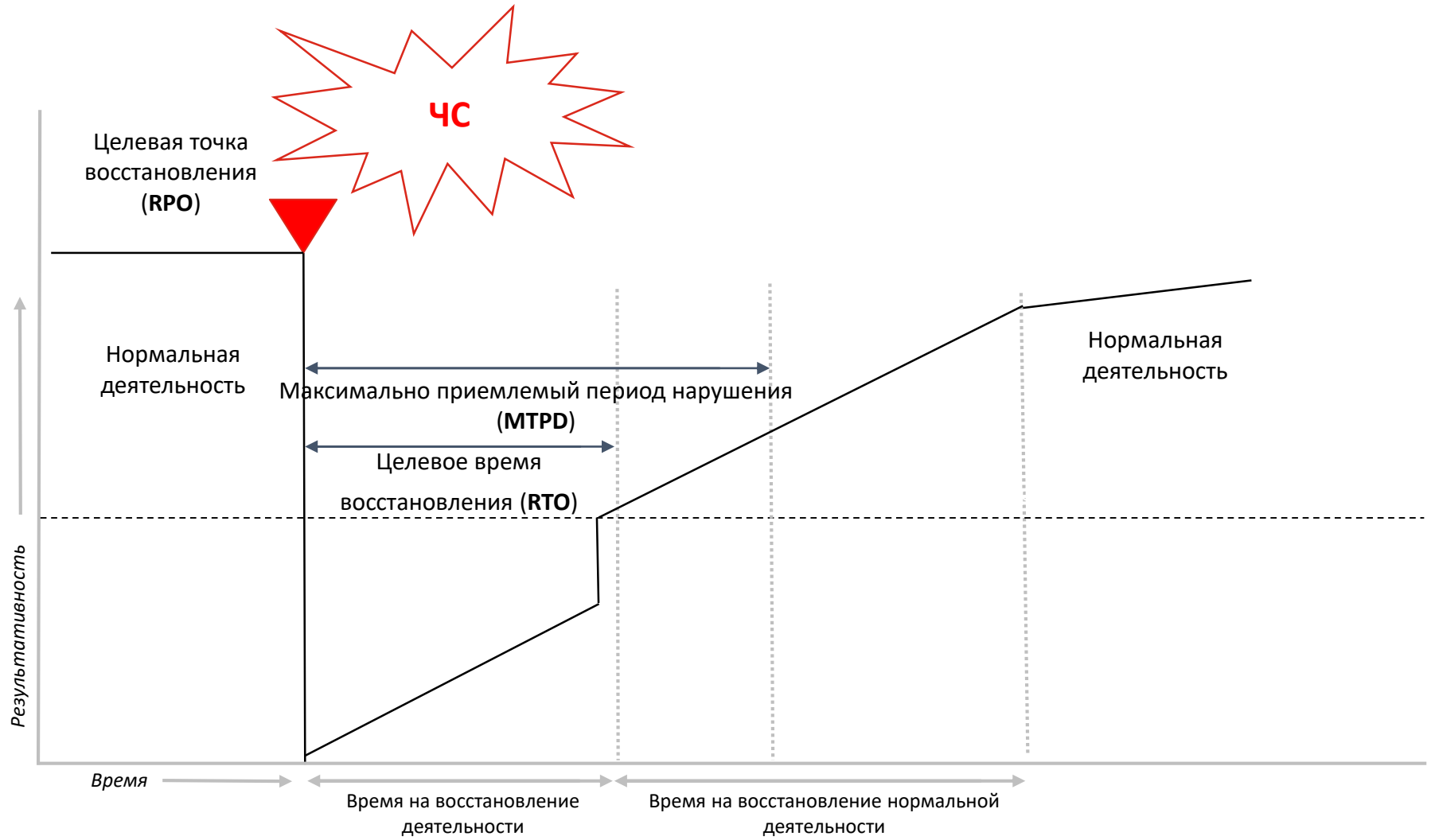
Идентификация ключевых бизнес-процессов



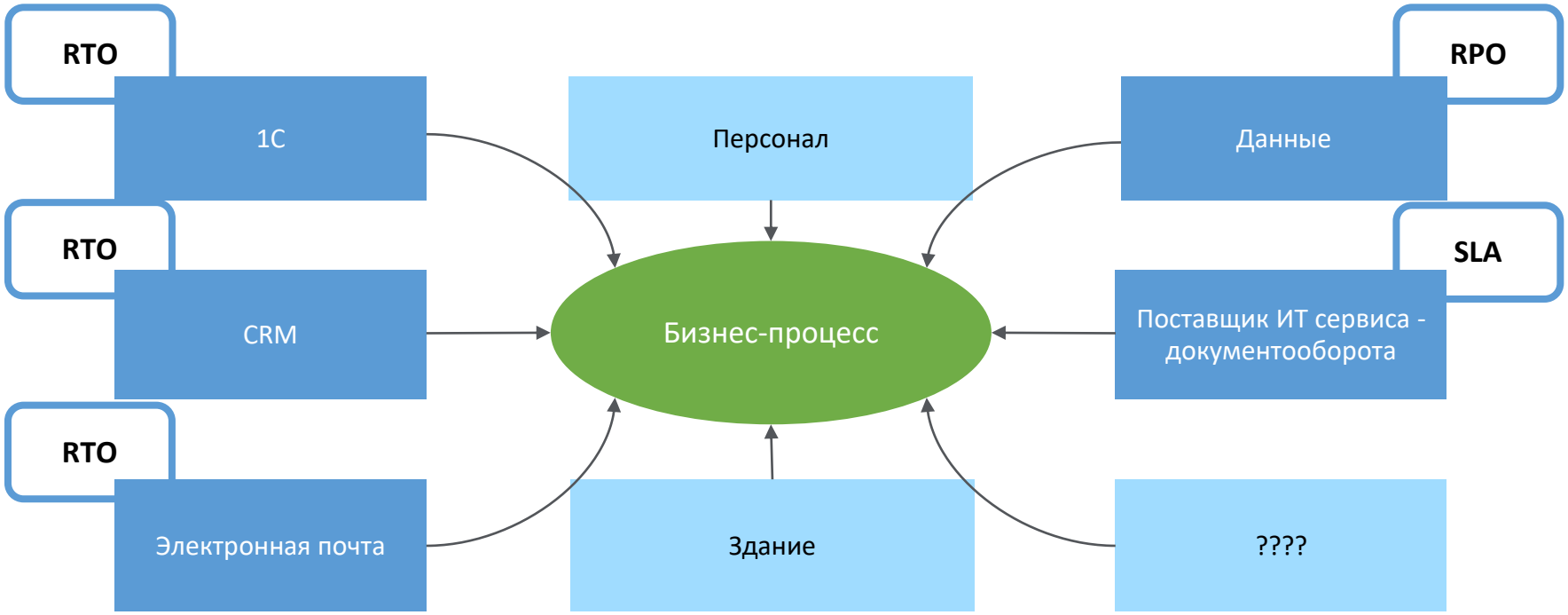
Подход к анализу воздействия на бизнес



Ключевые параметры непрерывности



Определение параметров непрерывности бизнеса



Пример результатов BIA

Пример 1

Бизнес процесс	ИТ ресурсы/ системы	Оценка критичности по временной шкале (RTO)												
		1 час	2 часа	3 часа	4 часа	5 часов	6 часов	7 часов	8 часов	9 часов	10 часов	11 часов	12 часов	24 часов
Процесс координации заявок	Система 1	5	4	4	4	4	3	3	3	3	3	3	3	3
	Система 2	4	4	3	3	2	2	2	1	1	1	1	1	1
	Система 3	4	4	3	3	2	2	2	1	1	1	1	1	1

Пример 2

Степень влияния	RTO	Процессы
Высокая	12 часов	Взаиморасчеты
	24 часов	Подача обязательной отчетности
Средняя	25–72 часа	Обработка финансовых транзакций Закрытие периода Консолидация Казначейские операции
Низкая	3–5 дней	Мониторинг цен
	1–5 недель	Налоговое администрирование и отчетность Комплайенс Управленческая отчетность

План обеспечения непрерывности бизнеса (BCP)

Угроза	Ресурс	Ответственный сотрудник	Превентивные меры	Действия во время сбоя	Время	Документация
Отсутствие доступа к ИТ компонентам	Сервер с БД	Иванов. И. И.	1. Создание резервной копии БД 2. Организация отказоустойчивого решения	1. Развертывание SQL-сервера 2. Восстановление из резервной копии 3. Активация БД утилитой	4 часа	1. Инструкция по установке и настройке 2. Инструкция по резервному копированию 3. Руководство администратора
Не приходят уведомления в системе	Сервер со службой	Сидоров А.А.	1. Создание резервной копии настроек службы 2. Развертывание службы быстрого запуска	1. Развертывание службы на новом сервере 2. Восстановление файла настроек 3. Перезапуск службы	30 мин	1. Инструкция по установке и удалению системы
Проблемы с загрузкой ОС	Сервер с БД	Иванов. И. И.	1. Создание резервной копии или точки восстановления ОС	1. Выполнение отката до точки восстановления 2. Удаление некорректного ПО	30-40 мин	1. Инструкции разработчика системного ПО
Некорректная работа приложений и ПО	Сервер со службой	Сидоров А.А.	1. Резервная копия каталога 2. Резервная копия файла настроек 3. Организация отказоустойчивого решения	1. Выполнение отката до точки восстановления 2. Удаление некорректного ПО	10-90 мин	1. Руководство администратора

План восстановления данных после аварии (DRP)

Период	Ответственный сотрудник	Действия время сбоя	Документация
1-ый день	Иванов. И. И.	1. Проверить работу всех необходимых приложений и в случае обнаружения ошибок в работе ПО, сообщить об этом работникам Блока информационных технологий. 2. Проверить степень завершения операций, завершить не выполненные. 3. Уведомить контрагентов о наступлении ЧС и о начале работы в условиях резервного офиса. 4. В случае остановки передачи электронных сообщений (ЭС), записать ЭС на USB Flash Drive и доставить в Нац Банк.	1. План обеспечения непрерывности и восстановления деятельности организации. 2. Инструкция о порядке восстановления передачи электронных каналов связи. 3. Инструкции по восстановлению штатной деятельности организации.
2-ой день	Сидоров А.А.	1. Организовать ввод 2-х сменного режима работы, обеспечив общую продолжительность работы департамента с 07.30 до 23.00. 2. Наладить обмен информацией на бумажных носителях (в случае необходимости) с контрагентами. 3. Восстановить штатную деятельность – осуществлять все необходимые операции.	
3-ий – 5-ый день	Иванов. И. И.	1. Настройка работы подразделения в режиме близком к штатному функционированию. 2. Уведомить контрагентов о временной смене адреса.	
6-ой – 10-ый день и далее	Сидоров А.А.	1. Организовать нормальное (штатное) функционирование подразделения. 2. Установить сохранность документов, касающихся деятельности подразделения и обязательных к хранению на бумажных носителях. 3. В случае утраты бумажных версий документов, инициировать работу по их восстановлению.	

Deloitte.