Риски и вызовы проектов по внедрению ПО для управления операционной надежностью по 787-П и 779-П ЦБ РФ в кредитных и некредитных финансовых организациях.

Илья Теодорович Лозинский

Группа Компаний Ланселот

LANCELOT
information technologies

LANCELOT
information technologies

- **Решения для управления операционными рисками финансовых и кредитных организаций по 716-П и 744-П.**
- **Решения для управления операционной надежностью по 787-П и 779-П.**
- **Внедрение аналитических приложений и систем делового интеллекта (BI).**

LANCELOT
information technologies

НАШИ ПРОЕКТЫ

ОАО БАНК «ОТКРЫТИЕ»	Внедрение системы СУОР в Банке Открытие
ОАО «ТРАНСКРЕДИТБАНК»	Внедрение системы в Транскредитбанке
ОАО «КОММЕРЧЕСКИЙ БАНК «ПЕТРОКОММЕРЦ»	Внедрение системы в Петрокоммерце
ОАО БАНК «ОТКРЫТИЕ»	Внедрение системы Служба клиентской поддержки, источник данных для СУОР
ОАО БАНК «ОТКРЫТИЕ»	Внедрение системы комплаенс «Конфликт интересов», источник данных для СУОР

LANCELOT
information technologies

LANCELOT
information technologies

ОАО БАНК «ОТКРЫТИЕ»	Внедрение подсистемы Аналитического анкетирования(самооценка), источник данных для СУОР
ОАО «НОМОС-БАНК»	Интеграция с АБС Номос-Банка
ОАО БАНК «ОТКРЫТИЕ»	Внедрение системы гибких классификаций и стоимостных оценок, расчет КИР
ОАО «НОМОС-БАНК»	Внедрение системы СУОР в Номос-банке
БАНК ВТБ	Внедрение системы Оценка факторов кредитного риска в ВТБ
АО «БКС БАНК»	Внедрение Аналитической витрины для событий СОР в БКС

LANCELOT
information technologies

LANCELOT
information technologies

Наши клиенты с ПО и ВНД для управления операционными рисками и операционной надежностью по 716-П , 787-П/779-П в 2021/2022 г.г.

SBI Bank
Strategic Business Innovator

citibank

Яндекс Деньги

Toyota Bank

MITSUBISHI MOTORS
Надежно.

MC Bank Rus
a subsidiary of Mitsubishi Corporation

РН Банк

БАНК ДОЛИНСК

БКС

БЕЛГОРОДСОЦБАНК
С нами всегда надежно!

ICBC

中国工商银行
INDUSTRIAL AND COMMERCIAL BANK OF CHINA

LANCELOT
information technologies

Наш бэкграунд:

Наше ПО рекомендовано компанией Ernst and Young как отечественное ПО для 716-П

ООО Ланселот – вендор № 1 на рынке ПО и консалтинга по 716-П в России в 2021 году

Мы единственный российский вендор с 10-летним опытом внедрения Систем Управления Операционным Риском (СУОР) и методологии управления операционными рисками

Часть 1: Сквозные технологические процессы

LANCELOT
information technologies

787-П/779-П: Обеспечение операционной надежности Технологических процессов

- Технологический процесс, обеспечивающий привлечение денежных средств физических лиц во вклады
- Технологический процесс, обеспечивающий привлечение денежных средств юридических лиц во вклады
- Технологический процесс, обеспечивающий размещение привлеченных во вклады денежных средств физических и (или) юридических лиц от своего имени и за свой счет
- Технологический процесс, обеспечивающий осуществление переводов денежных средств по поручению физических лиц по их банковским счетам
- Технологический процесс, обеспечивающий осуществление переводов денежных средств по поручению юридических лиц, в том числе банков-корреспондентов, по их банковским счетам, за исключением переводов по распоряжениям участников платежной системы
- Технологический процесс, обеспечивающий открытие и ведение банковских счетов физических лиц
- Технологический процесс, обеспечивающий открытие и ведение банковских счетов юридических лиц
- Технологический процесс, обеспечивающий осуществление переводов денежных средств без открытия банковских счетов, в том числе электронных денежных средств (за исключением почтовых переводов)
- Технологический процесс, обеспечивающий выполнение операций на финансовых рынках
- Технологический процесс, обеспечивающий выполнение кассовых операций
- Технологический процесс, обеспечивающий работу онлайн-сервисов дистанционного обслуживания и доступа к осуществлению операций
- Технологический процесс, обеспечивающий размещение и обновление биометрических персональных данных в единой биометрической системе
- Технологический процесс, обеспечивающий идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, в том числе с применением информационных технологий без их личного присутствия

LANCELOT information technologies

Риски и вызовы проектов по 787-П/779-П:

- 787-П и 779-П требуют организованного взаимодействия оперрисков, ИБ и ИТ безопасности, а так же СВА, СВК и ЦБ РФ .
- Не все процессы описаны. Часть описания процессов не актуальна. Нет владельцев процесса. Нет понимания, что «Сквозной процесс это не ИТ-Система».
- События по процессам в разных ИТ-системах либо не ведутся, либо ведутся частично и/или не консолидируются.
- Коллеги из смежных подразделений не знакомы с методологией 716-П (КИРы, лимиты, отчетность перед ЦБ).
- У них не прописана мотивация на обеспечение требований 716-П.

LANCELOT information technologies

LANCELOT
information technologies

Почему SLA - это не ответ на вызовы 787-П/779-П?

LANCELOT
information technologies

Сквозной процесс – это не только ИТсистема:

ПОЖАР В ОТЕДЕЛЕНИИ НЕ ПРИВОДИТ К СБОЮ В РАБОТЕ ИТ СИСТЕМ, НО ПРИВОДИТ К СБОЮ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА

"Технологический процесс, обеспечивающий привлечение денежных средств физических лиц во вклады"

Часть 1: Заключение

Ключевой компонент системы управления операционной надежностью это Модуль управления процессами

Часть 2: Параметры операционной надежности процессов

Риски и вызовы проектов по 787-П/779-П:

Как определить начальные параметры надежности процесса?

Относительно чего мерить?

Пример:

Считаем ли простоем технологическое окно?

Риски и вызовы проектов по 787-П/779-П:

Почему не валидно выводить SLA по ИТ системе?

Пример:

Для АБС стоит надежность 99% и плановое время восстановления после сбоя 2 часа.

При этом:

Для восстановление платежных сервисов – 2 часа слишком много.

НО:

Для комплайенс операций типа «Подтверждение наличия документов» – 2 часа или 24 часа это допустимое время.

ВЫВОД: Поэтому требуется опускаться до подпроцессов.

Почему не валидно выводить SLA по ИТ-системе: Связанные процессы (Лимит Сверху)

Например:

Сбой почтового сервиса и SMS нотификации влияет на большинство процессов.

Если он восстанавливается 6 часов, а лимит на восстановление платежного сервиса 2 часа – возможность платить будет восстановлена только через 6 часов т.к. без SMS не получится войти в личный кабинет.

Риски и вызовы проектов по 787-П/779-П:

ВЫВОД: SLA надо считать по процессу.

Нет линейной связи между доступностью ИТ-системы, ИБ сервиса, кибербезопасностью и сквозными процессами управления операционной надежностью.

Это не позволяет вести управление операционной надежностью в Excel или др. таблицах.

Часть 2: Заключение

Управление процессами подразумевает управления событиями, активами и рисками связанных подпроцессов

Часть 3: Методология операционной надежности процессов

Риски и вызовы проектов по 787-П/779-П: ВНД

Почему изменения ОНИВД не достаточно для выполнения требований 787-П/779-П?

Риски и вызовы проектов по 787-П/779-П:

Вызовы в разрезе отчетности по 787-П/779-П перед ЦБ РФ в части ВНД:

1. Необходимо кроме времени простоя отчитываться о количестве операций, которые не прошли (например биржевые трансакции, прием депозитов, внешние платежи).

2. Нужна Методика определения количества банковских операций, осуществляемых в рамках технологического процесса, осуществляемая в рамках его сбоя.

ВЫВОД: Необходимо утвердить методологию во Внутренних Нормативных Документах.

ВЫЗОВЫ 787-П/779-П в части методологии и ВНД:

Политика по ИБ это тоже не все

Нужны:

Порядок управления инцидентами информационной и кибербезопасности

+

Методика управления инцидентом

Зачем: Как определить критерии восстановления процесса после сбоя по ИБ и киберриску?

Часть 3: Вывод

Без Методологии невозможно управлять операционной надежностью процессов

Часть 4: Методология обеспечения полноты данных системы – ключевой компонент управления операционной надежностью процессов

Риски и вызовы проектов по 787-П/779-П: ВНД и интеграции

Система мониторинга простоев для обеспечения полноты и достоверности данных в рамках Методики обеспечения полноты данных должна определять Время простоя автоматически

Поэтому по каждой системе должны быть разработана:

План восстановления деятельности ИТ системы

+

Периодический Тест по Восстановлению Деятельности (в зависимости от критичности системы) *

*Тестируется не только время восстановления, но и система мониторинга и оповещения. Время восстановления фиксируется автоматически в системе мониторинга по доступности сервиса. Так время восстановления фиксируется по времени отклика владельцев процесса.

LANCELOT
information technologies

Риски и вызовы проектов по 787П/779П: ВНД 21+

1. Политика управления операционным риском.
2. Политика управления риском информационных систем.
3. Политика управления риском информационной безопасности.
4. Порядок обеспечения непрерывности и качества функционирования информационных систем.
5. Порядок и методы определения потерь от реализации событий операционных рисков, а также способов возмещения.
6. Система КПУР.
7. Положение об оценке персонала.
8. Система мотивации персонала к участию в управлении операционным риском.
9. Порядок ведения базы событий риска информационной безопасности Банка.
10. Порядок управления рисками информационной безопасности в Банке.
11. Концепция о применимости мер защиты информации в отношении объектов информационной инфраструктуры Банка.
12. Требования к организации ресурсного (кадрового и финансового) обеспечения системы обеспечения информационной безопасности Банка.
13. Обеспечении информационной безопасности на стадиях (этапах) жизненного цикла автоматизированных банковских систем Банка.
14. Методические указания к порядку расчета и обоснованию сигнальных и контрольных значений контрольных показателей уровня риска информационной безопасности Банка.
15. Организация контроля за функционированием системы обеспечения информационной безопасности Банка.
16. Сканирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры Банка.
17. Защита от воздействия вредоносных кодов Банка.
18. Положение об оценке СУОР.
19. Положение о порядке обнаружения, анализа и реагирования на инциденты, связанные с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств в Платежной Системе Банка.
20. Положение о порядке использования в ОАО внешних информационных систем.
21. План ОНиВД.

Часть 5: Компоненты системы управления операционной надежностью процессов

LANCELOT information technologies

ВЫЗОВЫ: Требования 787-П/779-П vs 716-П:

- **Реестр и конструктор процессов для обеспечения непрерывности выполнения критически важных процессов**
- Контрольные показатели уровня операционного риска
- **База событий реализованных рисков сбоев операционной надежности**
- Мониторинг непревышения значений порогового уровня допустимого времени простоя и (или) нарушения технологических процессов
- **Целевые показатели операционной надежности в разрезе процессов**
- **Контроль лимитов деградации процессов (в соответствии с пп. 4 787-П)**
- Контроль значений по КПУРам
- Учет и контроль параметров инцидента УОН

LANCELOT information technologies

LANCELOT information technologies

Требования 78-7П/779-П:

- **Оценка последствий рисков уязвимостей (Оценка потенциальных рисков уязвимостями в критичной архитектуре (в соответствии с пп. 6.2), которые корректируют значений целевых показателей операционной надежности)**
- **Планирование и внедрение мероприятий митигации риска**
- **Ведение базы рисков в части выявления, регистрации инцидентов операционной надежности и реагированию на них, а также восстановления выполнения технологических процессов и функционирования объектов информационной инфраструктуры после реализации таких инцидентов**
- Проведение сценарного анализа и тестирования готовности противостоять реализации информационных угроз в отношении критичной архитектуры
- **Контроль выполнения мер в зависимости от уровня опасности**
- Формирование отчетности для Банка России

LANCELOT information technologies

LANCELOT
information technologies

Система управления операционной надежностью по 787-П/779-П:

Рецепт работающей системы управления операционной надежностью это автоматизированное управление всеми процессами, связанными с ними активами и инцидентами, а так же рисками + закрепленная в ВНД методология.

Система управления операционной надежностью по 787-П/779-П:

Основной критерий эффективности:

Мгновенный автоматический запуск мер для минимизации последствий сбоя процесса, восстановления деятельности и профилактики таких сбоев в будущем.

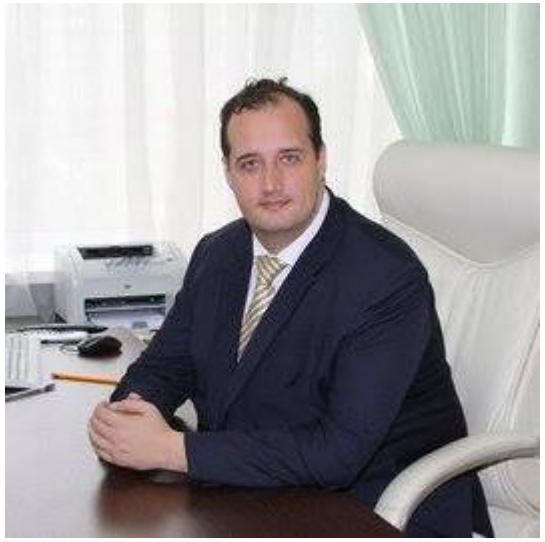
Наш опыт:

10 внедрений ПО СУОР и 6 проектов разработки ВНД для 716-П в 2021 г. в российских и иностранных банках

1. Услуга восстановления базы событий оперрисков на основании данных АБС, HelpDesk, CRM, SIEM, базы служебных записок и других IT систем.
2. Оперативная формализация и описание процессов 1-ого, 2-ого и 3-его уровня для решения проблемы «Есть положение по ОНиВД, но нет разбивке по процессам».
3. Описание критичности процессов для ОНиВД за 1 месяц.
4. Опыт разработки КИР и КПУР и лимитов по ним.
5. Методика анализа эффективности системы управления операционными рисками и операционной надежностью по 574 точкам.
6. Использование ВНД из банков, которые уже прошли проверки ЦБ РФ.
7. Сформированная система KPI для всех сотрудников для внедрения 716-П/78-7П/779-П.

LANCELOT
information technologies

Контакты:



Илья Теодорович Лозинский PhD, MBA

Управляющий партнер

ООО Ланселот

+ 7 499 380 7423

+7 925 963 7300

lozinsky@lancelot-it.ru

LANCELOT
information technologies