Грабли в ИБ или как наладить процессы по операционной надежности в НФО

АО ВТБ Специализированный депозитарий
Луганцев Александр
lugantsev@vtbsd.ru

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

П О Л О Ж Е Н И Е

«15» ноября 2021 г. № 779-П

г. Москва

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 67961
от "28" марта 2022.

Об установлении обязательных для некредитных финансовых организаций требований к операционной надежности при осуществлении видов деятельности, предусмотренных частью первой статьи 76[1] Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)», в целях обеспечения непрерывности оказания финансовых услуг (за исключением банковских услуг)

Настоящее Положение на основании статьи 76[4-2] Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» (Собрание законодательства Российской Федерации, 2002, № 28, ст. 2790; 2021, № 1, ст. 53), части 1 статьи 12 Федерального закона от 20 июля 2020 года № 211-ФЗ «О совершении финансовых сделок с использованием финансовой платформы» (Собрание законодательства Российской Федерации, 2020, № 30, ст. 4737), части 15 статьи 5, части 11 статьи 10 Федерального закона от 31 июля 2020 года № 259-ФЗ «О цифровых финансозых активах, цифровой валюте и о внесении изменений в отдельные

некредитными финансовыми организациями, указанными в абзаце первом пункта 1.2 настоящего Положения, обязанными соблюдать усиленный или стандартный уровень защиты информации в соответствии с подпунктом 1.4.2 или 1.4.3 пункта 1.4 Положения Банка России от 20 апреля 2021 года № 757-П, а также некредитными финансовыми организациями, не указанными в абзаце первом пункта 1.2 настоящего Положения, – с 1 октября 2022 года;

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

Методические рекомендации
по управлению риском информационной безопасности и обеспечению операционной надежности

21.03.2024 № 7-МР

Настоящие Методические рекомендации разработаны в целях обеспечения единства подхода к реализации кредитными организациями, за исключением центрального контрагента в значении, установленном пунктом 17 статьи 2 Федерального закона от 7 февраля 2011 года № 7-ФЗ «О клиринге, клиринговой деятельности и центральном контрагенте», и центрального

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 57580.3—2022

Безопасность финансовых (банковских) операций

УПРАВЛЕНИЕ РИСКОМ РЕАЛИЗАЦИИ ИНФОРМАЦИОННЫХ УГРОЗ И ОБЕСПЕЧЕНИЕ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

Общие положения

Издание официальное

Москва
Российский институт стандартизации
2023

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 57580.4—2022

Безопасность финансовых (банковских) операций

ОБЕСПЕЧЕНИЕ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

Базовый состав организационных и технических мер

Издание официальное

Москва
Российский институт стандартизации
2023

67 вопросов по реализации 779 - П

Создание рабочей группы по реализации 779 - П

Назначение ответственно по реализации 779 - П

Разработка организационно-распорядительной документации

Назначение ответственных (15 процессов)

- за разработку технологических процессов (определение состава и порядка выполнения технологических процессов);
- учет работников, осуществляющих физический и (или) логический доступ к информационным системам;
- оценку риска операционной надежности при функционировании технологически процессов, предусмотренных положением Банка России 779 – П;
- определение целевых показателе операционной надежности;
- регистрацию событий операционного риска;
- учет объектов информационной инфраструктуры, задействованных при выполнении каждого технологического процесса;
- учет каналов передачи защищаемой информации;
- планирование и внедрение изменений в критичной архитектуре;
- управление уязвимостями и обновлениями в критичной архитектуре;
- планирование и внедрение изменений в критичной архитектуре (в части предъявления требований по информационной безопасности);
- моделирование угроз информационной безопасности;
- проведение сценарного анализа;
- управление риском возникновения зависимости обеспечения операционной надежности от субъектов доступа - работников, обладающих знаниями, опытом и компетенцией, которые отсутствуют у всех иных работников;
- за обеспечение контроля соблюдения требований к операционной надежности;
- за выполнение мероприятий по реагированию на события операционного риска.

Ввод в действие ОРД

1. Положение по операционной надежности….;
- Положения 779 – П адаптированные к Организации;

Приложения к Положению:
- **Описание основных технологических процессов Общества;**
- Организационная структура Общества задействованная в выполнении требований к операционной надежности;
- Перечень инцидентов защиты информации и инцидентов операционной надежности Общества и составляющих их технологических процессов;
- Перечень каналов передачи защищаемой информации Общества;
- Методика расчета показателей операционной надежности Общества;
- Реестр технологических процессов, технологических участков технологических процессов, реализуемых поставщиками услуг в Обществе;
- Перечень программных сервисов, осуществляющих логический доступ к объектам информационной инфраструктуры Общества;

2. Положение по проведению оценки угроз безопасности информации в Обществе.

1. Оценка целей реализации нарушителями УБИ.
2. Результат определения актуальных нарушителей при реализации УБИ и соответствующие им возможности (в виде отдельного файла).
3. Определения актуальных способов реализации УБИ и соответствующие им виды нарушителей и их возможности.
4. Формирование группы реагирования на инциденты информационной безопасности и проведению экспертной оценки при оценке угроз безопасности информации.
5. Рекомендуемая структура модели УБИ.
6. Перечень нереализуемых угроз безопасности информации.
7. Описание возможных сценариев реализации угроз безопасности информации.

Описание технологических процессов Общества

Определение объектов информационной инфраструктуры Общества

1.1.Перечень объектов информационной инфраструктуры Компании задействованных в выполнении технологических процессов

Перечень информационных ресурсов Компании и их владельцев представлен в таблице № 1.

Таблица № 1. Перечень информационных ресурсов Компании

Приложение (информационный ресурс)	Функциональность	Владелец информационного ресурса	Пользователи информационного ресурса	Уровень критичности*
Система ДУ ОДК	Информационные системы разработки АО ВТБ Специализированный депозитарий предназначенные для проведения финансовых операций, организации взаимодействия с Клиентами Компании	Руководитель Управления обслуживания ипотечного покрытия и инвестиционных фондов	ЦУСЭДО УРиРПО УОИИ УДО ОРК УУиО УОИПиИФ	высокая
Регистратор ПИФ (Зенит)				высокая
Система СДУ ОДК				высокая
Система СДУ ОДК2		Руководитель Управления депозитарного обслуживания		высокая
		Руководитель Управления обслуживания институциональных инвесторов		высокая
ИС «Аналитика»	ИС представляет фондам и УК информацию в различных разрезах по их активам по портфелям, по операционным дням, в разрезе классов активов, информацию о справедливой стоимости.			высокая
Аванкор: Специализированный депозитарий	ИС для автоматизированной загрузки информации сервисов Интерфакса (RUDATA, RD FOR), полуавтоматическая интеграция с ЭДО	Руководитель Управления обслуживания ипотечного покрытия и инвестиционных фондов	УОИПиИФ	высокая
Модернизированная АС "Аванкор: Паевые фонды 3"			УОИПиИФ	высокая
XBRL	Автоматизированная подготовка отчетности по стандартам Банка России		СВК УОИИ	малая

Определение информационных ресурсов Компании и их функция в обеспечении выполнения технологических процессов

№ п/п	Функции ВТБ СД	Приложение (информационный ресурс)							WEB-сервисы	
		ОДК	ЭДО	Зенит	1С Аванкор	XBRL	1С	ЛУЧ	Система Аналитика	Личный кабинет УК ПИФ
1	Обслуживание пенсионных накоплений	x								
2	Пенсионных резервов НПФ	x								
3	Паевых инвестиционных фондов	x		x	x					
4	Ипотечного покрытия	x								
5	Страховых компаний	x								
6	Саморегулируемых организаций	x								
7	Государственных корпораций/компаний	x								
8	Депозитарные услуги	x								
9	Отправка отчетности в ЦБ	x	x			x				
10	Отправка отчетности в ЦБ по собственной деятельности						x			

Схема движения информационных потоков технологических процессов операционных подразделений в Компании

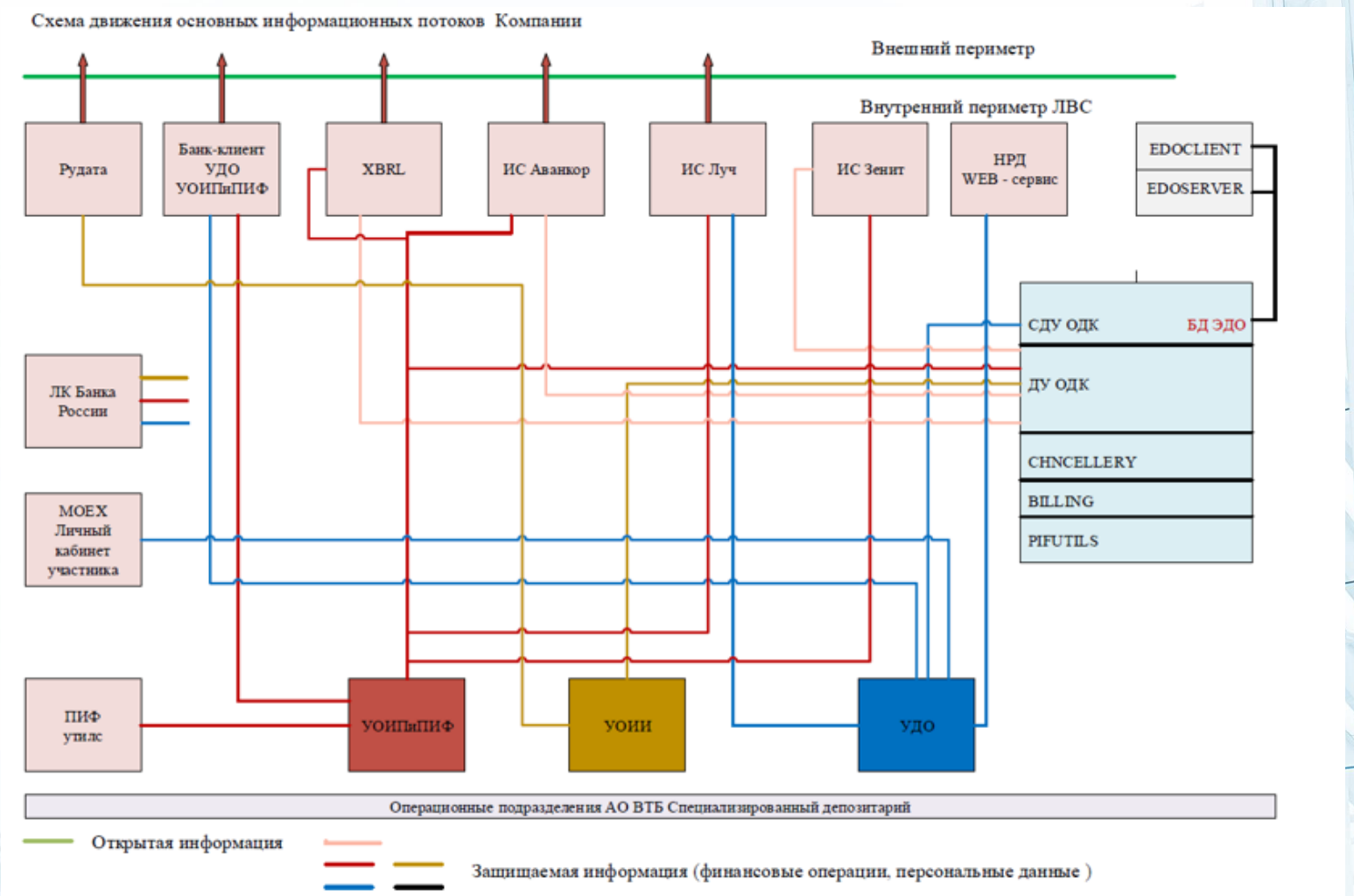
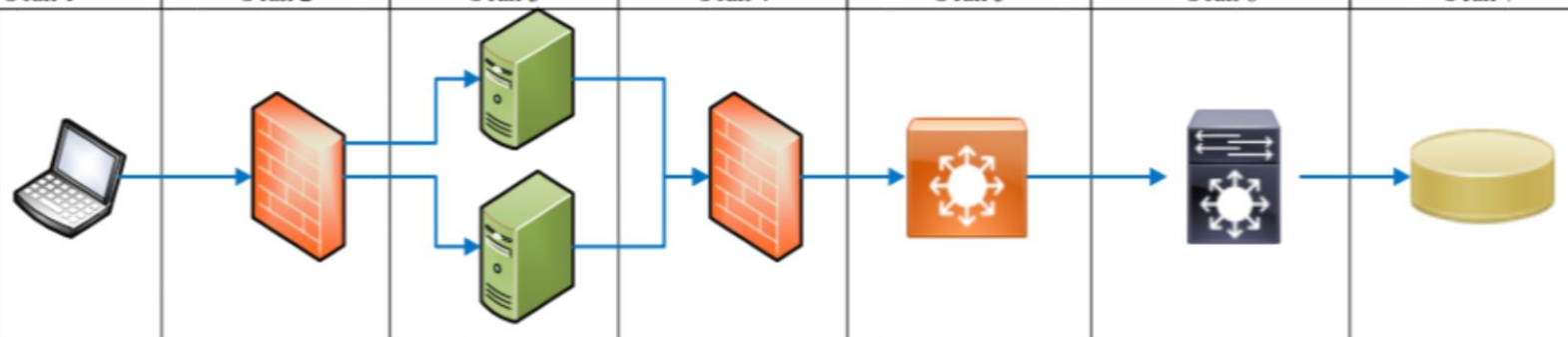


Схема движения информации при реализации технологических процессов с использованием системы электронного документооборота

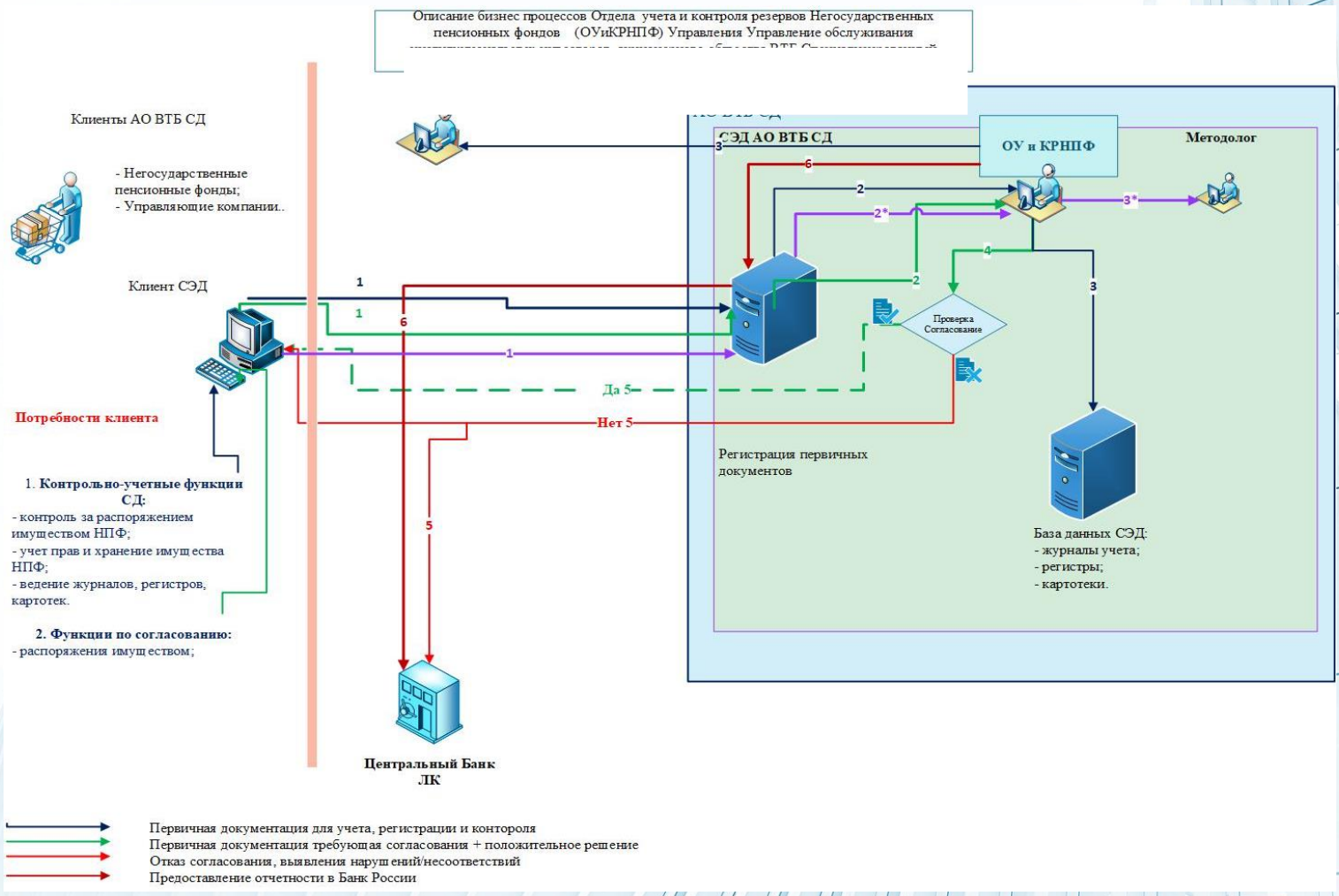
Логическая схема движения информации при реализации технологических процессов с использованием системы электронного документооборота



	Этап 1	Этап 2	Этап 3	Этап 4	Этап 5	Этап 6	Этап 7
Наименование	Рабочее место клиента	NGFW	Почтовый сервер Шлюз ЭДО SED.VTBSD.RU: 8080	UTM	Коммутатор ядра сети	Сервер ЭДО ЭДО 25	База данный СЭД
Функция (назначение)	Подготовка и направление первичной документации	Средство защиты информации для входящего информационного трафика	Прием/отправление первичной информации (типизированных форм) от клиентов	Средство защиты информации для внутреннего информационного трафика	Устройство обеспечивают общую коммутацию информационных потоков и сетей	Обработка поступающих от клиентов информационных сообщений (расшифровка/ зашифровка, обеспечение взаимодействия с базой данных)	Учетная система системы ЭДО Общества

Описание технологических процессов и их **взаимосвязь** с информационными системами других организаций и другими ТП

Краткое описание процессов функционирования подразделения, выполняемые задачи, каким образом подразделение задействовано в выполнении бизнес/технологических процессов

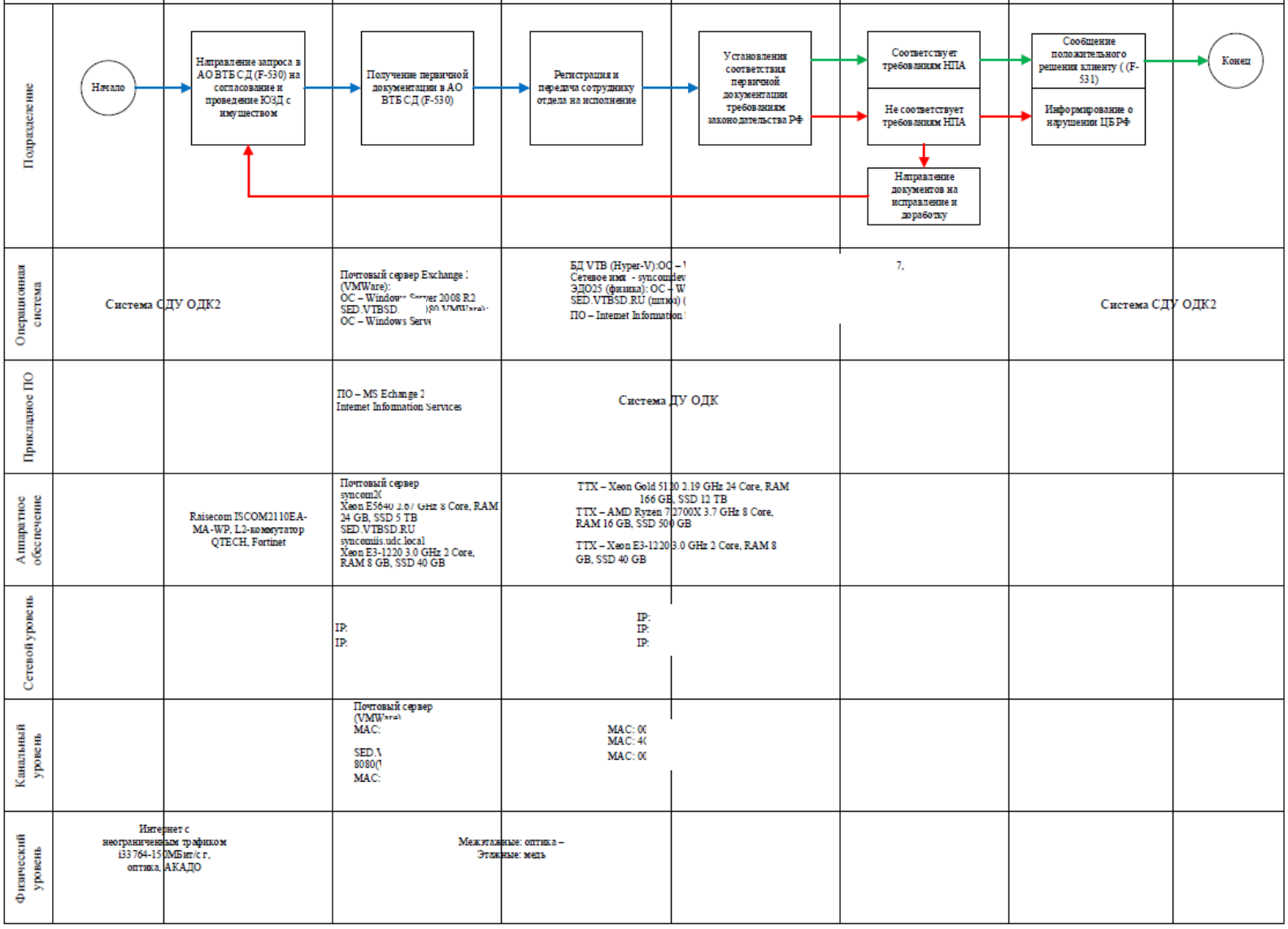


Перечень технологических участков технологического процесса

№ п/п	Наименование технологического участка	Участники (подразделения), обеспечивающие работоспособность технологического участка	ИС обеспечивающие работоспособность технологического участка	Примечание
1.	Идентификация, аутентификация и авторизация клиентов в целях осуществления финансовых операций.	1. Клиент – авторизация в клиентской части ЭДО. 2. ОЭТПС – обеспечение работоспособности каналов передачи информации, почтовых серверов. 3. ЦУСЭДО – обеспечение аутентификации пользователя в системе ЭДО.	1. Система СДУ ОДК.	Происходит в клиентской части программного обеспечения
2.	Формирование (подготовка), передача и прием электронных сообщений.	1. Клиент - формирование первичной документации и ее отправка). 2. ОЭТПС – обеспечение работоспособности каналов передачи информации, почтовых серверов. 3. ЦУСЭДО – обеспечение работоспособности транспортного уровня передачи электронных сообщений.	1. Система СДУ ОДК2. 2. Почтовый сервер	
3.	Удостоверение права клиентов распоряжаться денежными средствами,	1. ЦУСЭДО – обеспечение валидности выданных сертификатов ключей электронной подписи.	1. КриптоПро CSP. 2. ПАК "УЦ КриптоПро УЦ»	

Схема технологического процесса при контроле за распоряжением имуществом фондов и задействованных ПАК

Технологический процесс, обеспечивающий осуществление Отделом учета и контроля накоплений Негосударственных пенсионных фондов и Пенсионного фонда Российской Федерации контроля за распоряжением имуществом фондов



2.2.1. Перечень объектов информационной инфраструктуры задействованных при выполнении технологических процессов в Управлении обслуживания институциональных инвесторов.

Таблица№ 5. Перечень объектов информационной инфраструктуры УОИИ

Перечень объектов информационной инфраструктуры УОИИ				
Система СДУ ОДК				
Программное обеспечение				
№ п/п	Наименование ПО	Вендор/ производитель	Функционал	Вид ПО
1	СДУ ОДК	ВТБ СД	Реализация полнофункционального специализированного депозитарного учета по следующим направлениям: - Пенсионный фонд РФ; - Негосударственные пенсионные фонды; - Паевые инвестиционные фонды; - Саморегулируемые организации и государственные корпорации; - Страховые компании; - Ипотечное покрытие;	Прикладное ПО
Аппаратное обеспечение				
№ п/п	Наименование оборудования		Назначение	Примечание
1	E5640 2.67 GHz 8 Core, RAM 24 GB, SSD 5 TB		Виртуальный сервер. Обеспечение работоспособности почтового сервера.	
Сетевое оборудование				
№ п/п	Наименование		Назначение	Примечание
1		-MA-WP	Коммутационное оборудование провайдера (управляемый коммутатор)	
2			Коммутационное оборудование (L - 2 коммутатор)	
3			Коммутатор ядра сети	
4		12XGT 4SFP+ Switch	Межэтажный коммутатор	
Средства мониторинга и защиты информации				
№ п/п	Наименование	Производитель	Назначение	Примечание
Перечень вспомогательных информационных систем, используемых в УОИИ				
1	ЛК Банка России		Отправка сообщений о выявленных нарушениях и ежедневной отчетности по ПФР 10_4.	

2.2.2. Взаимосвязи и взаимозависимости между Управлением обслуживания институциональных инвесторов кредитными организациями и поставщиками услуг в рамках выполнения технологических процессов

Взаимодействие участников технологического процесса происходит в соответствии с установленными в Обществе Регламентами [1]в процессе осуществления контроля за:

- распоряжением средствами пенсионных резервов и средствами пенсионных накоплений;
- составом и структурой активов, в которые размещены средства пенсионных резервов и инвестированы средства пенсионных накоплений.

Взаимосвязи и взаимозависимости отражены в таблице№ 6.

Таблица № 6. Взаимосвязи и взаимозависимости в рамках выполнения технологических процессов

№ п/п	Наименование организации	Характер взаимосвязи/взаимозависимости	Примечания
1	Клиенты Управления (управляющие компании СФР, управляющие	Направляют в уполномоченный Банк и специализированный депозитарий для согласования: - платежные поручения на перечисление (списание) денежных средств с банковских счетов управляющих компаний СФР, управляющих компаний НПФ, НПФ с приложением соответствующих документов, в случае необходимости; - платежные распоряжения с приложением	

Для каждой информационной системы определяем критическое время простоя и связанные с этим риски

Время		Уровень тяжести последствий	Последствия негативного события, повлекшего выход из строя используемой информационной системы
Длительность простоя ИС	Наступление негативного события		
ИС ODKOFFISE			
	утро (до 12-00)	0	Практически нет влияния на процессы
1 час	день (до 18-00)	3	Задержки в обработке документов. Клиентский негатив ввиду задержки обработки документов (далее - везде)
	вечер (до 24-00)	3	Неадекватный контроль (задержка расчета СЧА – базы контроля). Проблемы с выявлением нарушений и обработкой данных об устранении ранее совершенных и уведомлением Банка России
	утро (до 12-00)	2	Невозможность предоставления первичных документов клиентом. Невозможность предоставления отчетности в Банк России (ежедневная/ежемесячная). Отсутствие возможности согласования текущих операций клиента и операций предыдущего дня
12 часов	день (до 18-00)	2	Смещение времени обработки операций, проблемы со сверкой (Т-) и проведением согласований операций за предыдущий день. Риски несвоевременного выставления нарушений и направления уведомлений об устранении
	вечер (до 24-00)	2	Неадекватный контроль (задержка расчета СЧА). Проблемы с выявлением нарушений и обработкой данных об устранении ранее совершенных и уведомлением Банка России
	утро (до 12-00)	1	Невозможность предоставления первичных документов клиентом. Невозможность предоставления отчетности в Банк России (ежедневная/ежемесячная). Отсутствие возможности согласования операций клиента и операций предыдущих дней
1 сутки	день (до 18-00)	1	Смещение времени обработки операций, нарушение ежедневности сверки, отсутствие возможности проведения согласования операций. Несвоевременное выставление нарушений и уведомлений об устранении.
	вечер (до 24-00)	1	Неадекватный контроль (задержка расчета СЧА). Проблемы с выявлением нарушений и обработкой данных об устранении ранее совершенных и уведомлением Банка России
Более суток		1	Лицензионный риск (неисполнение лицензируемого вида деятельности)

Мероприятия по обеспечению отказоустойчивости информационных систем, задействованных в обеспечении функционирования технологических процессов.

Резервное копирование информационных ресурсов.

Обеспечение отказоустойчивости аппаратных средств, задействованных в обеспечении функционирования технологических процессов.

Управление изменениями критичной архитектурой.

Управление уязвимостями и обновлениями в критичной архитектуре.

Планирование и внедрение изменений, управление конфигурациями в критичной архитектуре.

Управление доступом и предоставление полномочий.

Организационная структура подразделений Общества задействованной в выполнении требований к операционной надежности.

Рабочая группа по внесению изменений в 779 - П

Внесено – 50 предложений.
ВТБ СД – 28.
Учтено – 16.

Спасибо за внимание!