DIRECTUM. План обеспечения непрерывности бизнеса

Назначение и область применения

Данный документ описывает методику построения плана обеспечения непрерывности бизнеса, с учетом рекомендаций ITIL. План позволяет минимизировать влияние неблагоприятных событий на систему электронного документооборота(СЭД) DIRECTUM, и, как следствие, на бизнес заказчика.

Наличие в организации плана непрерывности бизнеса позволит снизить вероятность наступления неблагоприятных событий, а в случае их возникновения минимизировать время и стоимость простоя ИТ-сервисов, в том числе СЭД DIRECTUM.

Терминология, обозначения и сокращения

ITIL (IT Infrastructure Library) – библиотека, описывающая лучшие из применяемых на практике способов организации работы ИТ-подразделений или ИТ-компаний. Библиотека ITIL не является стандартом и носит только рекомендательный характер.

ITSCM (IT Service Continuity Management) – управление непрерывностью услуг, процесс, ответственный за управление рисками, которые влияют на услуги. ITSCM позволяет поставщику услуг постоянно предоставлять минимально согласованный уровень услуг, через снижение рисков до приемлемого уровня и планирование восстановления услуг.

ИТ-актив – материальные и нематериальные компоненты ИТ-инфраструктуры, в том числе аппаратное и программное обеспечение ИТ-систем и сервисов.

ИТ-сервис – ИТ-услуга, которую компания предоставляет клиентам для поддержки их бизнес-процессов.

Неблагоприятное событие – событие, результатом которого будет неработоспособное состояние системы в целом или ее отдельных частей.

Стоимость простоя – величина, определяемая как сумма составляющих недополученной прибыли от внепланового простоя системы, расходов на заработную плату пользователей, не работающих во время простоя, расходов на заработную плату ИТ-персонала, устраняющего причины простоя, а также потерь в репутации компании.

Этапы построения плана непрерывности бизнеса

Предлагаемая методика построения плана непрерывности бизнеса содержит три основных этапа:

- **Анализ рисков неблагоприятных событий**. Кратко этот блок можно охарактеризовать вопросом: «Что может произойти?». На выходе этого блока должна быть сформирована таблица с основными угрозами и соответствующими рисками для каждого ИТ-актива;
- **Мероприятия для снижения рисков**. Кратко этот блок можно охарактеризовать вопросом: «Что нужно сделать, чтобы риски не наступили?». На выходе этого блока должен быть разработан список плановых мероприятий для снижения вероятности проявления рисков неблагоприятных событий;
- **Мероприятия по восстановлению**. Кратко этот блок можно охарактеризовать вопросом: «Что делать, если риск все же наступил?». На выходе этого блока должен быть разработан план мероприятий по восстановлению сервисов в случае наступления неблагоприятного события, с написанием рабочих инструкций и порядком действий в каждой ситуации и для каждой угрозы.

Анализ рисков неблагоприятных событий

В первую очередь при написании плана обеспечения непрерывности бизнеса выполняется анализ списка возможных рисков, присущих конкретной организации, и степень воздействия этих рисков на бизнес.

Риски можно разделить на следующие подгруппы:

- риски, оказывающие влияние на ИТ-активы, и, как следствие, на доступность сервиса;
- риски, возникающие при обслуживании сервиса.

Рассмотрим порядок анализа рисков каждой группы.

Риски, оказывающие влияние на ИТ-активы

Данные риски связаны с возникновением любых нештатных ситуаций с ИТ-активами при ежедневной эксплуатации ИТ-сервиса.

1. **Список ИТ-активов.** Первоначально необходимо составить список всех ИТ-активов влияющих на доступность ИТ-сервиса.
2. **Список угроз.** Для каждого ИТ-актива определяются угрозы, то есть список негативных внешних воздействий, могущих привести к недоступности этого актива.

   Все угрозы, затрагивающие ИТ-активы (ИТ-инфраструктуру) можно классифицировать по следующим группам:
   - атмосферные явления (наводнения, землетрясения, снегопады);
   - техногенные аварии (отключение электричества, отключение отопления, пожар);
   - действия третьих лиц (ограбление, умышленная порча оборудования);
   - отказ оборудования, как оборудования ИТ-инфраструктуры, так и оборудования, обеспечивающего ее нормальное функционирование (отказ системы кондиционирования серверной);
   - отказ отдельных сервисов и служб, влияющих на всю систему в целом (для СЭД DIRECTUM это будет отказ SQL-службы, утеря БД, неработоспособность сервера сеансов и т.д.).
3. **Вероятность наступления угрозы.** Для каждой угрозы определяется величина угрозы, то есть вероятность ее наступления. Она может быть оценена по статистическим данным либо субъективно.
4. **Уязвимость ИТ-актива к угрозам.** Далее для каждого ИТ-актива определяется его уязвимость по отношению к угрозам. Это означает степень влияния внешнего фактора на общий ИТ-сервис при воздействии этого фактора на данный ИТ-актив. Обычно высокая уязвимость ИТ-актива связана с тем, что он является единой точкой сбоя в процессе предоставления ИТ-услуги. Например, если один источник питания обслуживает кластер серверов, содержащий критичную информацию для бизнеса, то уязвимость такого источника питания будет максимальной по отношению к отключению электричества.
5. **Расчет степени риска.** Наступление угрозы в любом ИТ-активе означает определенный вид нарушения ИТ-сервиса в целом, например недоступность технического персонала, потеря данных, полное разрушение ИТ-систем (в случае глобальных угроз), недоступность сети и т. д. Возможность подобных нарушений идентифицируется в качестве рисков, связанных с ИТ-сервисом в целом.

Степень риска = (Вероятность угрозы) x (Уязвимость актива)

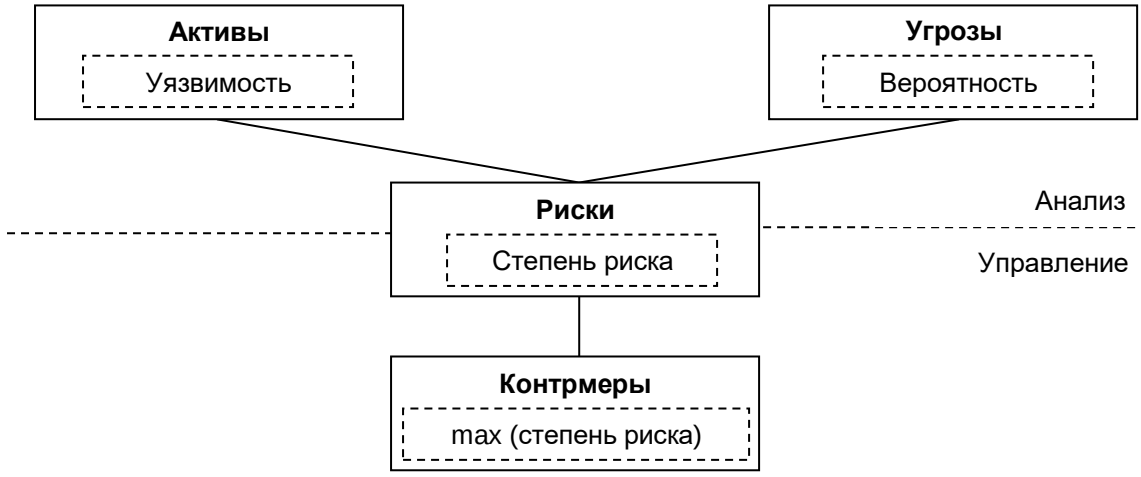
Таким образом, степень риска ИТ-сервиса определяется как произведение вероятности угрозы на уязвимость актива по отношению к этой угрозе. Определение степени риска приведено в таблице 1.

Таблица 1. Определение степени риска

Уязвимость \ Угроза	Высокая	Средняя	Низкая
Высокая	**Максимальная**	Высокая	Средняя
Средняя	Высокая	Средняя	Низкая
Низкая	Средняя	Низкая	Незначительная

Количество оцененных рисков для каждого ИТ-сервиса может быть очень велико, поэтому часто пользуются правилом Top 10, когда рассматриваются лишь первые десять самых распространенных рисков.

Идентификация и оценка степени - это первый шаг к управлению рисками. Управлять рисками означает принимать меры по уменьшению вероятности и степени воздействия риска и быть готовым к кризисным ситуациям в случае их наступления.



6. **Итоговая таблица со степенями риска.** После проведения анализа соответствия активов и угроз для всех компонент системы, для каждой компоненты формируется таблица зависимости степеней риска от уязвимостей и угроз.

   Например, в СЭД DIRECTUM наиболее критичными являются следующие компоненты системы (от наиболее к наименее критичным):

   - база данных SQL Server;
   - сервер сеансов;
   - служба WorkFlow;
   - службы файловых хранилищ (если они присутствуют);
   - прочие модули и компоненты системы, используемые в организации и на которые завязаны критичные бизнес-процессы (определяется в каждой конкретной организации индивидуально). Например, сервер веб-доступа будет одной из наиболее критичных компонент, в организации, где большая часть пользователей, имеют доступ к системе исключительно через веб-доступ.

От работоспособности этих компонент зависит функционирование системы в целом. Определим степень критичность риска для некоторых из них:

Таблица 2. Пример определения зависимости степени риска от уязвимостей и угроз

Угроза (неблагоприятное событие)	Вероятность наступления	Актив	Уязвимость	Степень риска (из таблицы 1)	Примечание
Наводнение	Низкая	Сервер с БД DIRECTUM	Высокая	**Средняя**	
Наводнение	Низкая	Сервер с WorkFlow	Средняя	**Низкая**	
Отказ оборудования	Средняя	Сервер с БД DIRECTUM	Высокая	**Высокая**	
Отказ оборудования	Средняя	Сервер с сервером сеансов	Высокая	**Высокая**	

Риски, возникающие при обслуживании сервиса

Данные риски связаны с самим ИТ-сервисом, его развитием, обновлением и поддержанием работоспособности. Следующие действия могут быть причиной наступления рисков данного вида:

- плановые работы по обслуживанию (замене или ремонту) аппаратной части;
- действия, связанные с установкой обновлений системного программного обеспечения (обновление ОС, драйверов, СУБД);
- действия, связанные с обновлением прикладного ПО, в том числе обновление или конвертация системы на новую версию.

Аналогично рискам, оказывающим влияние на ИТ-активы, необходимо провести анализ и составить таблицу зависимостей степеней риска от угроз.

Плановые мероприятия для снижения рисков

Превентивные меры

После того как составлена таблица основных угроз с высокими и максимальными степенями риска для ИТ-сервиса, разрабатывается список плановых мероприятий по недопущению возникновения данных угроз. В этот список должны входить мероприятия, рекомендуемые производителем аппаратной части и разработчиком программного обеспечения.

Список должен содержать меры уменьшения риска, а выполнение действий из этого списка должно носить регулярный характер.

Угрозы никогда нельзя устранить полностью. При этом важно учитывать, что уменьшение одного вида риска может привести к увеличению другого.

К превентивным мерам, снижающим риски на ИТ-активы, можно отнести:

- обеспечение отказоустойчивости систем с критичными приложениями, для которых неприемлем любой простой;
- инсталляция источников бесперебойного и резервного питания для серверов и прочего оборудования, предназначенного для сохранения основной ИТ-инфраструктуры организации;
- использование избыточных массивов жестких дисков на серверах для снижения вероятности аппаратного сбоя и, как следствие, потери информации;
- наличие запасных компонентов/оборудования, которые будут использованы в случае сбоя основных. Например, запасной сервер с минимально необходимой конфигурацией, который будет задействован в кратчайшее время в случае отказа основного сервера;
- устранение единых точек отказа, например единой точки доступа в сеть или единой точки электропитания.

К превентивным мерам, снижающим риск при обслуживании ИТ-сервиса, можно отнести:

- выдача минимально необходимых прав на выполнение действий в системе и максимальное ограничений круга лиц, имеющих привилегии администратора;
- регулярная установка протестированных обновлений и различных исправлений, влияющих на безопасность;
- всеобъемлющая стратегия восстановления и резервного копирования, включающая в себя внешнее хранение. Внешнее хранение предполагает регулярное (чаще всего ежедневное) копирование критичной информации во внешнее хранилище.
- увеличение контроля над обнаружением нарушений в работе услуг;
- увеличение контроля над безопасностью, в том числе шифрование данных, аудит и т.д.;
- выполнение действий по обслуживанию, обновлению и модификации ИТ-сервиса строго в соответствии с инструкциями производителя. Изначально этот пункт должен выполняться на тестовой среде и только после успешного завершения – на рабочей, с возможностью отката всех изменений.

Мониторинг

Основой предотвращения неблагоприятного события служит постоянный мониторинг показателей производительности и доступности ИТ-сервиса в целом. Мониторинг на ранних стадиях позволяет обнаружить и определить возможные неблагоприятные события, как в оборудовании системы, так и в инфраструктуре в целом.

Определяется список метрик для каждого события в таблице 2 (какой-то конкретный счетчик, событие в лог-файле и т.д.), за которыми будет производиться наблюдение и их постоянный анализ.

Так, например, в качестве системы мониторинга может использоваться система System Center Operation Manager (SCOM), Zabbix, либо система подобного класса для enterprise-предприятий.

Мероприятия по восстановлению сервисов в случае неблагоприятного события

Восстановление

В случае если неблагоприятное событие произошло, и мероприятия, направленные на минимизацию последствий, не оказали соответствующего влияния, необходимо разработать план по восстановлению сервисов в случае аварий для каждой из угроз, определенных в таблице 2.

Целью данного плана является быстрое восстановление ИТ-сервиса в работоспособное состояние, с минимальным временем простоя.

Вместо создания отдельных, частных инструкций и руководств, удобнее всю информацию представить в едином документе. Пример плана по восстановлению предоставлен в приложении 1.

План восстановления должен содержать:

- описание набора конкретных шагов и действий;
- среднее время, выделенное для выполнения каждого действия;
- команда исполнителей, задействованных на данном шаге.

Детальные планы восстановления оформляются как официальные документы компании. Любые изменения в них необходимо согласовывать со всеми заинтересованными сторонами, принимающими участие в процессе восстановления.

План восстановления должен включать все виды работ, связанных с предоставлением услуг во время чрезвычайной ситуации. В плане также должны быть определены процедуры, необходимые для его выполнения, эффективные и понятные настолько, чтобы каждый специалист мог выполнять работы по восстановлению, следуя этим процедурам.

Согласно рекомендациям ITIL, под восстановлением подразумевается не только собственно восстановление, но и предоставление дополнительных дублирующих систем на время ремонта основного ИТ-сервиса, или так называемого обходного решения, которые обеспечат непрерывность предоставления ИТ-услуг.

Варианты восстановления в рамках ITSCM, которые должны быть учтены при формировании плана:

- переход на альтернативные варианты функционирования служб в период восстановления, например, учет заявок в службу снабжения (службу поддержки) в бумажном журнале;
- постепенное восстановление (Gradual Recovery) - способ восстановления, также известный как "холодное резервирование". Предусматривается восстановление услуги в течение более чем 72 часов. При постепенном восстановлении обычно задействован мобильный или стационарный резервный центр. Этот вариант восстановления рекомендован для некритичных услуг, предоставление которых может быть задержано на дни и недели без значительного влияния на бизнес;
- промежуточное восстановление (Intermediate Recovery) - способ восстановления, также известный как "теплое резервирование". Предусматривается восстановление услуги в течение 24 - 72 часов. При промежуточном восстановлении обычно используется общий мобильный или стационарный резервный центр, оснащенный компьютерными системами и сетевыми компонентами. Конфигурирование аппаратного и программного обеспечения, а также восстановление данных выполняются в рамках Плана обеспечения непрерывности услуг. Стоимость этого варианта восстановления зависит от ресурсов третьей стороны, которые

должны быть задействованы для восстановления, а также от времени, в течение которого требуется восстановить услугу. Преимуществом данного метода является его прозрачность для пользователей. Недостатком - то, что информация (в том числе конфиденциальная) будет храниться у сторонней организации. Последнее делает неприемлемым данный способ восстановления для многих организаций.

- быстрое восстановление (Fast Recovery) -.Предусматривается восстановление услуги за короткий промежуток времени, обычно менее 24 часов. При быстром восстановлении обычно используется выделенный стационарный резервный центр с компьютерными системами и ПО, сконфигурированными для работы услуг. Немедленное восстановление может занимать до 24 часов, если требуется восстановление данных резервного копирования.
- немедленное восстановление (Immediate recovery) - способ восстановления, также известный как "горячее резервирование". Предусматривается восстановление услуги без прерывания услуги. Немедленное восстановление обычно использует технологии зеркалирования, балансировки загрузки и разделения площадок установки оборудования. Этот способ чаще всего предусматривает "двойную локацию" компонентов системы, то есть полное дублирование. Он является самым дорогим и применяется только для критичных бизнес-процессов, простой которых может оказать значительное негативное влияние на бизнес. Копии должны быть расположены на максимальном удалении от оригиналов, чтобы не быть задетыми разрушающим событием.

Так, например, план по восстановлению системы DIRECTUM должен содержать:

- восстановление минимальной части модулей и компонент, необходимых для функционирования ИТ-сервиса (например, организация доступа в систему DIRECTUM), т.е. этому пункту соответствует вариант немедленного или быстрого восстановления, а также переход на альтернативные варианты функционирования;
- восстановление оставшейся части ИТ-сервиса (модулей и компонент), необходимой для полного и корректного функционирования всех бизнес-процессов организации. Данному пункту могут соответствовать все варианты восстановления.

Различные услуги, используемые организацией, требуют различных подходов к восстановлению и уменьшению рисков сбоя. Какие бы варианты ни выбирались, они должны быть экономически эффективны.

Тестирование

Планы по восстановлению должны проходить регулярное тестирование и актуализацию. Тестирование является важной частью ITSCM. Именно оно гарантирует то, что принятые стратегия, соглашения, планы и процедуры будут действительно работать на практике.

Поставщик услуг несет ответственность за то, что в случае катастрофы услуги могут быть восстановлены в заданный временной интервал с требуемой функциональностью и производительностью. Тесты должны проводиться по максимально реалистичным сценариям. При невозможности использования рабочей среды (серверов, БД и т.д.) тестирование проводится на тестовой среде. Тем не менее, необходимо понимать, что даже самое тщательное тестирование не может учесть все нюансы, которые могут возникнуть в реальности.

После выполнения тестов обязательным пунктом является актуализация всей документации, относящейся к восстановлению, и поддержание ее в актуальном состоянии.

Управление непрерывностью ИТ-услуг

Управление непрерывностью должно включать:

- Обучение, подготовка, тренинги – персонал должен быть готов к возникновению непредвиденных обстоятельств и знать, что необходимо делать при их возникновении;
- Пересмотр и аудит – возможное появление новых внешних угроз или автоматизация новых бизнес-процессов означает неизбежное изменение требований к имеющимся ключевым ИТ-сервисам. Регулярное обновление планов и процедур по обеспечению непрерывности ключевых ИТ-услуг позволит ИТ-подразделению гибко приспосабливаться к изменяющемуся бизнесу организации;

- Тестирование – помимо начального тестирования, необходимо предусмотреть регулярное тестирование стратегии, планов и других выходов ITSCM. Резервные копии и механизмы восстановления также должны тестироваться.

Приложение 1

Таблица 3. Пример плана основных действий при восстановлении системы (для версии DIRECTUM 4.9.1).

Пункт	Угроза	Актив	Имя сервера	Ответственный	Время выполнения *	Описание последствий	Превентивные меры	Краткое описание действий, выполняемых для восстановления системы	Ссылки на стандартную документацию	Примечание
1.	Отказ оборудования (перенос на новое оборудование)	Сервер с БД	server-db	Иванов И.И.	3 часа	Нет доступа ко всем компонентам системы DIRECTUM	1. Резервная копия БД 2. Организация отказоустойчивого решения	1. Развертывание SQL-сервера 2. Восстановление из резервной копии в соответствии со стратегией резервного копирования 3. Активация БД утилитой SASystemActivator.exe в режиме активации существующей системы 4. Регистрация системы DIRECTUM	1. Инструкция по установке и настройке Microsoft SQL Server 2. Инструкция по резервному копированию и восстановлению базы данных DIRECTUM 3. Инструкция по установке и удалению системы > Установка серверной части системы DIRECTUM 4. Руководство администратора > Установка системы DIRECTUM	
		Сервер со службой «Сервер сеансов»	server-ss	Иванов И.И.	15 мин.	Все пользователи не могут подключиться к системе (зайти в систему)	1. Резервная копия файла настроек службы SBSessionSrvSettings.xml 2. Развертывание службы на failover-кластере, для организации быстрого запуска, в случае сбоя	1. Развертывание службы «Сервер сеансов» на новом сервере 2. Восстановление файла настроек SBSessionSrvSettings.xml, перезапуск службы «Сервер сеансов» 3. Регистрация системы DIRECTUM	1. Инструкция по установке и удалению системы > Установка сервера сеансов системы DIRECTUM 2. Руководство администратора > Управление сервисными службами 3. Руководство администратора > Установка системы DIRECTUM	
		Сервер со службой Workflow	server-wf	Иванов И.И.	15 мин.	Не приходят задания и уведомления в системе DIRECTUM	1. Резервная копия файла настроек службы SBWorkflowSrvSettings.xml 2. Развертывание службы на failover-кластере, для организации быстрого запуска, в случае сбоя	1. Развертывание службы WorkFlow на новом сервере 2. Восстановление файла настроек SBWorkflowSrvSettings.xml, перезапуск службы WorkFlow	1. Инструкция по установке и удалению системы > Установка службы WorkFlow системы DIRECTUM	

Пункт	Угроза	Актив	Имя сервера	Ответственный	Время выполнения *	Описание последствий	Превентивные меры	Краткое описание действий, выполняемых для восстановления системы	Ссылки на стандартную документацию	Примечание
		Сервер со службой файловых хранилищ (ФХ)	server-dss	Иванов И.И.	15 мин.	Недоступна часть документов, не удается создать документы с некоторыми видами электронных документов	1. Резервная копия каталога с ФХ 2. Резервная копия файла настроек службы SBFileStorageSettings.xml 3. Организация отказоустойчивого решения	1. Развертывание службы ФХ на новом сервере 2. Восстановление файла настроек SBWorkflowSrvSettings.xml, перезапуск службы 3. Восстановление каталога из резервной копии 4. Инициализация ФХ в системе DIRECTUM	Руководство администратора > Развертывание файловых хранилищ	
2.	Некорректное обновление системного ПО (обновление ОС, драйверов и т.д.)	Сервер с БД	server-db	Петров П.П.	20-90 мин.	Проблемы с загрузкой ОС, некорректная работоспособность приложений и ПО	1. По возможности выполнение на тестовой среде 2. Резервная копия или точка восстановления ОС	Выполнение отката до точки восстановления либо удаление некорректного ПО	В соответствии с инструкциями разработчика системного ПО	
		Сервер со службой «Сервер сеансов»	server-ss	Петров П.П.	10-90 мин.		1. По возможности выполнение на тестовой среде 2. Резервная копия или точка восстановления ОС			
		Сервер со службой Workflow	server-wf	Петров П.П.	10-90 мин.		1. По возможности выполнение на тестовой среде 2. Резервная копия или точка восстановления ОС			
		Сервер со службой файловых хранилищ	server-dss	Петров П.П.	10-90 мин.		1. Резервная копия каталога с ФХ 2. Резервная копия файла настроек службы SBFileStorageSettings.xml 3. Организация отказоустойчивого решения			

Пункт	Угроза	Актив	Имя сервера	Ответственный	Время выполнения *	Описание последствий	Превентивные меры	Краткое описание действий, выполняемых для восстановления системы	Ссылки на стандартную документацию	Примечание
3.	Некорректное обновление системы DIRECTUM, в том числе незавершенная конвертация или конвертация выполнена с ошибками	Сервер с БД	server-db	Сидоров С.С.	30-60 мин.	Часть функционала системы DIRECTUM стала неработоспособна	1. Резервная копия БД 2. Обязательное выполнение на тестовой среде(базе) в соответствии с прилагаемой инструкцией по конвертации 3. Тестирование основных бизнес-процессов пользователями системы	1. Восстановление из резервной копии с помощью утилиты SASystemActivator.exe 2. Регистрация системы DIRECTUM	1. Инструкция по установке и удалению системы > Установка серверной части системы DIRECTUM 2. Руководство администратора > Установка системы DIRECTUM	
		Сервер со службой «Сервер сеансов»	server-ss	Сидоров С.С.	15-30 мин.	Все пользователи не могут подключиться к системе (зайти в систему)	1. По возможности выполнение на тестовой среде 2. Проверка наличия дистрибутивов для текущей (используемой) версии 3. Резервная копия файла настроек службы SBSessionSrvSettings.xml	1. Развертывание службы «Сервер сеансов», ранее используемой версии 2. Восстановление файла настроек SBSessionSrvSettings.xml, перезапуск службы «Сервер сеансов» 3. Регистрация системы DIRECTUM	1. Инструкция по установке и удалению системы > Установка сервера сеансов системы DIRECTUM 2. Руководство администратора > Управление сервисными службами 3. Руководство администратора > Установка системы DIRECTUM	
		Сервер со службой Workflow	server-wf	Сидоров С.С.	15-30 мин.	Не формируются задания по задачам	1. По возможности выполнение на тестовой среде 2. Проверка наличия дистрибутивов для текущей (используемой) версии 3. Резервная копия файла настроек службы SBWorkflowSrvSettings.xml	1. Развертывание службы WorkFlow, ранее используемой версии 2. Восстановление файла настроек SBWorkflowSrvSettings.xml, перезапуск службы WorkFlow	Инструкция по установке и удалению системы > Установка службы WorkFlow системы DIRECTUM	
		Сервер со службой файловых хранилищ	server-dss	Сидоров С.С.	15-30 мин.	Недоступна часть документов, не удается создать документы с некоторыми видами электронных документов, выводятся сообщения о несоответствии версий	1. По возможности выполнение на тестовой среде 2. Проверка наличия дистрибутивов для текущей (используемой) версии 3. Резервная копия файла настроек службы SBFileStorageSettings.xml	1. Развертывание службы ФХ, ранее используемой версии 2. Восстановление файла настроек SBWorkflowSrvSettings.xml, перезапуск службы	Руководство администратора > Развертывание файловых хранилищ	

* Время выполнения необходимо скорректировать после проведения тестовых развертываний, т.к. оно зависит от конфигурации аппаратного обеспечения, компетенций сотрудников, объема базы и других факторов.