УТВЕРЖДЕН

ПРОГРАММНЫЙ КОМПЛЕКС «ИРИДИУМ-VDI»

План аварийного восстановления

Листов 22

2026

Подп. и дата	
Инв. № дубл.	
Взам. Инв №	
Подп. и дата	
Инв. № подл.	

СОДЕРЖАНИЕ

1 ПЛАН АВАРИЙНОГО ВОССТАНОВЛЕНИЯ ПК «ИРИДИУМ-VDI»

1.1 Назначение документа

Настоящий документ определяет порядок подготовки, запуска и выполнения аварийного восстановления программного комплекса «Иридиум-VDI» после отказов программных и аппаратных компонентов, ошибок персонала, чрезвычайных обстоятельств, хакерских или вирусных атак.

План предназначен для администраторов и специалистов эксплуатации Заказчика. Процедуры сформированы таким образом, чтобы восстановление могло быть выполнено силами Заказчика без привлечения вендора Системы и без обращения в техническую поддержку Системы при наличии актуальных резервных копий, доступа к инфраструктуре и учетных данных администратора.

Целевой показатель восстановления: восстановление работы Системы для 6500 пользователей не более чем за 8 часов без деградации функционала платформы UTAG.

1.2 Термины и сокращения

Термин	**Описание**
VDI	Инфраструктура виртуальных рабочих столов
Система	ПК «Иридиум-VDI» и зависимые инфраструктурные сервисы, необходимые для предоставления пользователям виртуальных рабочих столов и приложений
BPM	Виртуальное рабочее место
RTO	Целевое время восстановления сервиса или компонента
RPO	Максимально допустимая потеря данных за период между последней резервной копией и аварией
DR	Аварийное восстановление
Резервная площадка	Инфраструктурная площадка, подготовленная для запуска сервисов при недоступности основной площадки

1.3 Область применения

План применяется при следующих событиях:

— отказ сервера VDI, контейнера VDI, базы данных, брокера подключений, VDI Actor, транспортного шлюза или клиентских компонентов;
— отказ гипервизора, хранилища, сетевой инфраструктуры, DNS, DHCP, LDAP/LDAPS, Active Directory или RDS;
— ошибочное удаление или изменение конфигурации, шаблонов BPM, пулов, поставщиков услуг, политик доступа;
— компрометация учетных записей, вредоносное воздействие, шифрование данных, нарушение целостности образов;
— пожар, затопление, отказ электропитания, недоступность серверной, недоступность основной площадки.

1.4 Требования и принципы аварийного восстановления

План аварийного восстановления должен обеспечивать непрерывность функционирования Системы за счет резервного копирования, документированных процедур диагностики, восстановления компонентов и переключения на резервную площадку.

План учитывает рекомендации и лучшие практики стандартов ISO 22301, ISO/IEC 27001, ISO/IEC 27002 и ISO/IEC 27031 в части управления непрерывностью деятельности, защиты информации, восстановления ИТ-сервисов и регулярной проверки готовности к аварийному восстановлению.

Основные принципы:

— приоритет восстановления задается критичностью компонента для запуска пользовательских сессий;
— восстановление выполняется по заранее утвержденным инструкциям;
— все действия фиксируются в журнале аварийного восстановления;
— перед восстановлением после кибератаки выполняется изоляция пораженного сегмента и проверка резервных копий;
— восстановление производится из последней доверенной резервной копии;
— после восстановления выполняется функциональная проверка Системы и проверка доступности для контрольной группы пользователей;

— возврат на основную площадку выполняется только после подтверждения стабильности основной инфраструктуры.

1.5 Роли и ответственность

Роль	**Ответственность**
Руководитель восстановления	Принимает решение о запуске плана, назначает ответственных, контролирует RTO, утверждает переключение на резервную площадку
Администратор VDI	Восстанавливает сервер VDI, контейнеры, конфигурацию, пулы, поставщиков услуг, транспортные настройки
Администратор платформы виртуализации	Восстанавливает гипервизор, кластеры, хранилища, шаблоны ВМ и виртуальные рабочие места
Администратор инфраструктурных сервисов	Проверяет и восстанавливает DNS, DHCP, LDAP/LDAPS, Active Directory, NTP, сертификаты
Администратор ИБ	Оценивает признаки компрометации, выполняет изоляцию, проверяет резервные копии и разрешает ввод восстановленных сервисов в эксплуатацию
Представитель эксплуатации	Проверяет доступность сервиса для пользователей и фиксирует завершение восстановления

1.6 Схема сервиса и зависимости

ПК «Иридиум-VDI» предоставляет пользователям доступ к виртуальным рабочим столам и приложениям через сервер VDI, брокер подключений, поставщиков услуг, службы аутентификации и платформу виртуализации.

Логическая схема зависимостей:

1) Пользовательское устройство подключается к порталу VDI или транспортному шлюзу.
2) Сервер VDI выполняет аутентификацию пользователя через LDAP/LDAPS или Active Directory.
3) Сервер VDI обращается к базе данных и получает сведения о правах, пулах, поставщиках услуг и доступных ВРМ.

4) Брокер VDI взаимодействует с поставщиком услуг: ПК «Иридиум», ПК «Иридиум», RDS или статические IP-машины.
5) Платформа виртуализации запускает или предоставляет ВРМ из пула.
6) VDI Actor передает состояние ВРМ и служебную информацию серверу VDI.
7) Пользователь подключается к ВРМ через настроенный протокол доставки: RDP, SPICE, NX, LoudPlay или иной разрешенный транспорт.

Критические зависимости приведены в таблице.

Компонент	**Зависит от**	**Влияние отказа**
Сервер VDI	ОС, Docker, контейнер VDI, база данных, сеть, DNS, сертификаты	Пользователи не могут пройти авторизацию и получить назначенные сервисы
База данных VDI	Том данных контейнера, хранилище, резервная копия	Потеря конфигурации, пулов, пользователей, поставщиков услуг
Поставщик услуг	Платформа виртуализации, учетная запись администратора, сеть	Невозможно создать, запустить или назначить ВРМ
Платформа виртуализации	Хосты, кластеры, СХД, сеть управления	Недоступны виртуальные рабочие места и шаблоны
VDI Actor	ОС ВРМ или RDS, сеть до сервера VDI	Некорректное определение состояния ВРМ и нарушение управления сессиями
Службы аутентификации	LDAP/LDAPS, AD, DNS, время, сертификаты	Пользователи и администраторы не могут войти в Систему
DNS/DHCP/NTP	Сетевые сервисы площадки	Нарушение разрешения имен, выдачи адресов и Kerberos/LDAPS-аутентификации
Транспортный шлюз	Сервер VDI, ВРМ, сертификаты, сетевые маршруты	Пользователи не могут подключиться к рабочим столам извне или через HTML5
Хранилище	СХД, сети хранения, репликация, снимки	Недоступны шаблоны, диски ВРМ, база данных и резервные копии

1.7 Целевые показатели восстановления

План предусматривает восстановление обслуживания 6500 пользователей в течение 8 часов. Для выполнения данного показателя должны быть заранее подготовлены:

— актуальные резервные копии сервера VDI, базы данных, томов контейнеров, шаблонов BPM, конфигурации поставщиков услуг и транспортных шлюзов;
— резервная инфраструктура или достаточный ресурс на основной площадке для повторного запуска компонентов;
— документированные сетевые параметры, DNS-записи, сертификаты и учетные данные;
— проверенные процедуры восстановления и контрольная группа пользователей для приемки.

Компонент	**RPO**	**RTO компонента**	**Примечание**
DNS, DHCP, NTP	24 ч	30 мин	Восстанавливаются первыми, если недоступны
LDAP/LDAPS, Active Directory	24 ч	1 ч	Требуются для входа пользователей и администраторов
Платформа виртуализации и хранилище	24 ч	2 ч	Должны предоставить ресурсы для сервера VDI и BPM
Сервер VDI и контейнеры	4 ч	1 ч	Восстановление ОС, Docker, контейнера и томов
База данных VDI	4 ч	1 ч	Восстановление конфигурации Системы
Поставщики услуг и пулы	4 ч	1 ч	Проверка связей с платформой виртуализации и RDS
Транспортные шлюзы и сертификаты	24 ч	1 ч	Требуются для внешнего доступа и HTML5
Шаблоны BPM, золотые образы	24 ч	2 ч	Восстановление или переподключение к хранилищу
Массовый запуск BPM для 6500 пользователей	24 ч	4 ч	Может выполняться параллельно после восстановления управления

Полное восстановление сервиса	4-24 ч	8 ч	Итоговый целевой показатель

1.8 Условия запуска плана

План запускается при наступлении одного или нескольких условий:

- недоступность пользовательского сервиса VDI более 15 минут и невозможность восстановления штатными действиями;
- отказ критического компонента без автоматического восстановления;
- повреждение или потеря конфигурации Системы;
- недоступность основной площадки;
- подтвержденная или предполагаемая компрометация сервера VDI, базы данных, хранилища или учетных записей;
- требование руководителя восстановления или ответственного за эксплуатацию.

Перед запуском плана необходимо зафиксировать:

- дату и время инцидента;
- признаки отказа;
- список затронутых компонентов;
- число затронутых пользователей;
- последние успешные резервные копии;
- принятое решение: восстановление на основной площадке или переключение на резервную.

1.9 Инструкция по резервному копированию

1.9.1 Общие требования

Резервное копирование должно выполняться регулярно, контролироваться средствами мониторинга и проверяться тестовым восстановлением не реже одного раза в квартал.

Резервные копии должны храниться минимум в двух независимых местах: на основной площадке и вне основной площадки или в изолированном хранилище. Для

защиты от вирусных и хакерских атак рекомендуется использовать неизменяемые копии или хранилище с запретом перезаписи в течение срока хранения.

Минимальная схема хранения:

— ежедневные копии за последние 14 календарных дней;

— еженедельные копии за последние 8 недель;

— ежемесячные копии за последние 12 месяцев;

— отдельная доверенная копия после каждого значимого изменения конфигурации.

1.9.2 Состав резервных копий

Объект	**Способ резервного копирования**	**Периодичность**	**Срок хранения**
ВМ или сервер VDI	Снимок/backup ВМ, копия ОС и системных настроек	ежедневно	14 дней
Docker-образ VDI	Экспорт образа или хранение исходного архива поставки	при обновлении	весь срок эксплуатации версии
Том данных VDI	Backup Docker volume или файловая копия с остановкой сервиса	каждые 4 часа	14 дней
База данных VDI	Логический дамп и/или физическая копия файлов БД	каждые 4 часа	14 дней
Конфигурация VDI	Экспорт настроек, скриншоты критичных параметров, выгрузки списков	ежедневно и после изменений	90 дней
Шаблоны BPM	Backup ВМ-шаблонов и золотых образов	ежедневно и после изменений	30 дней
Пулы и назначенные BPM	Резервная копия БД и экспорт описания пулов	каждые 4 часа	14 дней
VDI Actor	Дистрибутив, версия, параметры подключения к серверу VDI	при изменении	весь срок эксплуатации версии
Транспортный шлюз	Backup ВМ/контейнера, сертификаты, конфигурация маршрутов	ежедневно	30 дней

Сертификаты и ключи	Защищенная копия сертификатов, закрытых ключей и паролей	при выпуске/замене	до окончания срока действия
DNS/DHCP/LDAP/AD	Штатные средства backup соответствующего сервиса	ежедневно	по политике Заказчика
Журналы аудита	Экспорт в централизованное хранилище журналов	постоянно	по политике ИБ

1.9.3 Порядок резервного копирования сервера VDI

1) Проверить доступность сервера VDI по сети и наличие свободного места в целевом хранилище резервных копий.
2) Зафиксировать текущую версию контейнера VDI командой `docker images`.
3) Зафиксировать состояние контейнера командой `docker ps -a`.
4) Выполнить резервное копирование тома данных контейнера VDI штатным инструментом резервного копирования или командой, принятой в эксплуатационной документации Заказчика.
5) Выполнить логический дамп базы данных, если база данных используется как отдельный сервис.
6) Скопировать файл дампа, архив тома, сведения о версии контейнера и контрольные суммы в резервное хранилище.
7) Проверить успешность задания backup и отсутствие ошибок в журнале.
8) Записать результат в журнал резервного копирования.

1.9.4 Контроль резервных копий

После каждого задания backup необходимо проверить:

— статус задания резервного копирования;
— наличие файла резервной копии в целевом хранилище;
— размер файла и контрольную сумму;
— возможность чтения резервной копии;
— соответствие фактического RPO целевому значению;
— отсутствие предупреждений ИБ о компрометации источника резервной копии.

1.10 Инструкция по диагностике состояния компонентов Системы

1.10.1 Первичная диагностика

1) Проверить доступность портала VDI с рабочей станции администратора.
2) Проверить доступность сервера VDI по IP-адресу и DNS-имени.
3) Проверить состояние контейнера VDI командой `docker ps -a`.
4) Проверить журналы контейнера командой `docker logs <имя_контейнера> --tail 200`.
5) Проверить свободное место на дисках сервера VDI.
6) Проверить доступность базы данных и тома данных.
7) Проверить доступность LDAP/LDAPS или AD.
8) Проверить доступность платформы виртуализации и поставщиков услуг.
9) Проверить доступность DNS, DHCP, NTP и сетевых шлюзов.
10) Проверить события ИБ и признаки вредоносного воздействия.

1.10.2 Диагностика сервера VDI

Проверка	**Команда или действие**	**Ожидаемый результат**
Состояние ОС	Проверить загрузку CPU, RAM, дисков и сетевых интерфейсов	Нет исчерпания ресурсов
Docker	`docker info`	Служба Docker работает
Контейнер VDI	`docker ps -a`	Контейнер `star.vdi` запущен или доступен для запуска
Журналы VDI	`docker logs star.vdi --tail 200`	Нет повторяющихся критических ошибок
Порт сервиса	Проверить порт публикации контейнера	Порт доступен с рабочих мест администраторов
Том данных	Проверить наличие Docker volume или каталога данных	Том доступен и не поврежден

1.10.3 Диагностика базы данных

1) Проверить доступность сервиса базы данных.
2) Проверить наличие свободного места в хранилище базы данных.

3) Проверить журналы базы данных на ошибки повреждения таблиц, нехватки места и отказов подключения.
4) Проверить возможность подключения учетной записью сервера VDI.
5) Сравнить время последней успешной резервной копии с целевым RPO.

1.10.4 Диагностика поставщиков услуг

1) Войти в административную панель VDI.
2) Перейти в раздел поставщиков услуг.
3) Проверить статус поставщика ПК «Иридиум», ПК «Иридиум», RDS или статических IP-машин.
4) Выполнить тест подключения к поставщику, если функция доступна в интерфейсе.
5) Проверить учетные данные поставщика и срок действия пароля.
6) Проверить доступность API или консоли платформы виртуализации.
7) Проверить состояние хранилищ, кластеров и сетей, используемых пулами ВРМ.

1.10.5 Диагностика VDI Actor

1) Выбрать контрольное ВРМ из каждого типа пула.
2) Проверить запуск гостевой ОС.
3) Проверить состояние службы VDI Actor.
4) Проверить доступность сервера VDI с ВРМ.
5) Проверить открытость служебного порта Actor.
6) Проверить журналы Actor на ошибки регистрации, авторизации или связи.

1.10.6 Диагностика зависимых сервисов

Сервис	**Проверка**	**Критерий исправности**
DNS	Разрешение имен сервера VDI, AD, гипервизора, шлюзов	Имена разрешаются в корректные IP-адреса
DHCP	Выдача адресов ВРМ и клиентским устройствам	Адреса выдаются из корректных пулов
NTP	Синхронизация времени серверов VDI, AD и гипервизора	Расхождение времени не нарушает аутентификацию

LDAP/LDAPS/AD	Авторизация тестового пользователя	Успешный вход, сертификат LDAPS действителен
Хранилище	Доступность датасторов, LUN, NFS/iSCSI	Нет ошибок ввода-вывода
Сеть управления	Доступность API гипервизора и сервера VDI	Нет потерь пакетов и блокировок ACL
Сеть пользователей	Доступность портала и протоколов доставки	Пользователь может подключиться к BPM
Система мониторинга	Актуальность метрик и событий	Метрики поступают без задержек

1.11 Последовательность восстановления компонентов

Восстановление выполняется в следующем порядке:

1) Обеспечить безопасность: изолировать пораженные узлы, остановить распространение инцидента, сохранить журналы.
2) Восстановить базовую инфраструктуру: электропитание, сеть, маршрутизацию, DNS, DHCP, NTP.
3) Восстановить службы аутентификации LDAP/LDAPS или Active Directory.
4) Восстановить хранилище и платформу виртуализации.
5) Восстановить сервер VDI, Docker и контейнер VDI.
6) Восстановить базу данных и том данных VDI.
7) Восстановить поставщиков услуг и проверить связь с платформой виртуализации.
8) Восстановить шаблоны BPM, золотые образы и пулы.
9) Восстановить VDI Actor на шаблонных ВМ и RDS-серверах при необходимости.
10) Восстановить транспортные шлюзы, сертификаты и маршруты пользовательского доступа.
11) Выполнить массовый запуск BPM и проверку пользовательских подключений.
12) Перевести Систему в штатную эксплуатацию после приемочной проверки.

1.12 Инструкция по восстановлению сервера VDI

1) Подготовить сервер или ВМ с параметрами не ниже исходных.

2) Настроить сетевые параметры, имя узла, DNS, NTP и доступ к хранилищу.
3) Установить Docker версии, совместимой с используемой версией VDI.
4) Загрузить образ VDI из архива поставки или доверенного репозитория командой `docker load < <файл_образа>`.
5) Восстановить Docker volume или каталог данных из последней доверенной резервной копии.
6) Восстановить базу данных из дампа или физической копии.
7) Запустить контейнер VDI с параметрами, соответствующими исходной конфигурации, например:

```
docker run -d --name=star.vdi -p 2637:2637 --restart=always -v svdi.vol:/svol
star.vdi:<версия>
```

8) Проверить состояние контейнера командой `docker ps`.
9) Проверить журналы командой `docker logs star.vdi --tail 200`.
10) Проверить вход в административную панель VDI.
11) Проверить наличие пользователей, пулов, поставщиков услуг и настроек транспорта.

1.13 Инструкция по восстановлению базы данных VDI

1) Остановить контейнер VDI или перевести сервис в режим обслуживания.
2) Проверить целостность выбранной резервной копии и ее соответствие времени RPO.
3) Восстановить файлы базы данных или импортировать логический дамп.
4) Проверить права доступа к файлам базы данных и тому данных.
5) Запустить сервис базы данных.
6) Запустить контейнер VDI.
7) Проверить журналы на ошибки миграции схемы, отсутствия таблиц или некорректных прав.
8) Выполнить вход в административную панель и проверить ключевые сущности: поставщиков услуг, пулы, пользователей, политики и транспортные настройки.

1.14 Инструкция по восстановлению поставщиков услуг

1) Проверить доступность платформы виртуализации или RDS-инфраструктуры.

2) Проверить учетные данные поставщика услуг.
3) В административной панели VDI открыть раздел поставщиков услуг.
4) Для каждого поставщика выполнить тест подключения.
5) При ошибке подключения проверить адрес, порт, учетную запись, сертификаты и сетевые правила.
6) Если поставщик отсутствует после восстановления БД, создать его вручную по эксплуатационной документации и данным из резервной конфигурации.
7) Проверить доступность хранилищ, шаблонов и сетей, привязанных к сервисам.
8) Перевести поставщика из режима обслуживания после успешной проверки.

1.15 Инструкция по восстановлению пулов и виртуальных рабочих мест

1) Проверить наличие шаблонов BPM и золотых образов на хранилище.
2) Проверить настройки пулов в административной панели VDI.
3) Проверить назначение пользователей и групп.
4) Для сессионных пулов выполнить запуск контрольной группы BPM.
5) Для статических пулов проверить соответствие BPM назначенным пользователям.
6) Проверить наличие VDI Actor и доступность служебного канала связи.
7) При повреждении пула пересоздать пул из восстановленного шаблона и подключить пользователей согласно выгрузке конфигурации.
8) Выполнить поэтапный запуск BPM: сначала 50 тестовых пользователей, затем 10%, 25%, 50% и 100% расчетной нагрузки.

1.16 Инструкция по восстановлению VDI Actor

1) Проверить версию Actor, используемую в шаблонах BPM и на RDS-серверах.
2) Проверить наличие дистрибутива Actor в защищенном хранилище.
3) На контрольной машине проверить состояние службы Actor.
4) При повреждении переустановить Actor согласно руководству администратора VDI.
5) Указать корректный адрес сервера VDI.
6) Проверить связь Actor с сервером VDI.

7) Обновить шаблон BPM, если Actor устанавливался в шаблон.
8) Пересоздать или перезапустить BPM, зависящие от обновленного шаблона.

1.17 Инструкция по восстановлению транспортных шлюзов

1) Восстановить ВМ или контейнер транспортного шлюза из резервной копии.
2) Проверить сетевые интерфейсы, маршруты и правила межсетевого экранирования.
3) Восстановить сертификаты и закрытые ключи из защищенного хранилища.
4) Проверить доступность сервера VDI со стороны шлюза.
5) Проверить доступность контрольных BPM со стороны шлюза.
6) Проверить публикацию пользовательских портов и HTML5-доступа, если он используется.
7) Выполнить тестовое подключение пользователя через внешний контур.

1.18 Инструкция по восстановлению после хакерской или вирусной атаки

1) Изолировать подозрительные серверы, BPM и сегменты сети.
2) Запретить использование скомпрометированных учетных записей.
3) Сохранить журналы VDI, ОС, Docker, базы данных, AD, гипервизора, шлюзов и средств защиты.
4) Определить доверенную точку восстановления до момента компрометации.
5) Проверить выбранные резервные копии средствами антивирусной защиты и контроля целостности.
6) Развернуть восстановление в чистом сегменте или на резервной площадке.
7) Заменить пароли и ключи сервисных учетных записей.
8) Перевыпустить сертификаты при признаках компрометации закрытых ключей.
9) Проверить отсутствие признаков вредоносной активности после восстановления.
10) Разрешить подключение пользователей только после подтверждения администратора ИБ.

1.19 Инструкция по переключению на резервную площадку

Переключение на резервную площадку применяется, если основная площадка недоступна или восстановление на ней не позволяет уложиться в целевое время 8 часов.

Предварительные условия:

— на резервной площадке подготовлены вычислительные ресурсы, хранилище и сети для запуска VDI;
— настроена репликация или регулярная доставка резервных копий;
— подготовлены DNS-записи, IP-адреса, маршруты, правила межсетевого экранирования и сертификаты;
— выполнена проверка запуска контрольного пула BPM;
— обеспечена емкость для обслуживания 6500 пользователей без деградации функционала платформы UTAG.

Порядок переключения:

1) Руководитель восстановления принимает решение о переключении на резервную площадку.
2) Остановить автоматические задания, которые могут перезаписать резервные копии или реплики.
3) Зафиксировать последнюю доступную точку восстановления.
4) Запустить инфраструктурные сервисы резервной площадки: DNS, DHCP, NTP, LDAP/AD или каналы связи к ним.
5) Запустить хранилище и платформу виртуализации резервной площадки.
6) Восстановить сервер VDI, базу данных, контейнеры и транспортные шлюзы.
7) Проверить поставщиков услуг, пулы и шаблоны BPM.
8) Переключить DNS-записи или балансировщик на резервную площадку.
9) Проверить вход администратора и тестового пользователя.
10) Запустить массовое восстановление BPM для пользователей.
11) Уведомить эксплуатацию и пользователей о восстановлении сервиса.

Возврат на основную площадку выполняется отдельным регламентом после устранения причин аварии, синхронизации данных и тестового переключения.

1.20 Инструкция по проверке состояния Системы после восстановления

После восстановления необходимо выполнить приемочные проверки.

Проверка	**Критерий успешности**
Вход администратора	Администратор входит в панель VDI без ошибок
Вход пользователя	Тестовый пользователь проходит аутентификацию
Поставщики услуг	Все используемые поставщики доступны и проходят тест подключения
Пулы	Пулы отображаются, назначения пользователей сохранены
Запуск BPM	Контрольное BPM запускается из каждого критичного пула
Подключение к BPM	Пользователь подключается по штатному протоколу доставки
VDI Actor	Состояние BPM корректно передается в VDI
Транспортный шлюз	Подключение работает через внутренний и внешний контуры
Печать, USB, буфер обмена, звук	Функции доступны в соответствии с политиками
UTAG	Функционал платформы доступен без деградации
Мониторинг	Метрики и события поступают в систему мониторинга
Журналы	Ошибки критического уровня отсутствуют или обработаны
Производительность	Расчетная нагрузка 6500 пользователей обслуживается в пределах утвержденных показателей

1.21 Массовое восстановление обслуживания 6500 пользователей

Для выполнения требования восстановления за 8 часов используется поэтапный запуск:

1) Восстановить управляющие компоненты VDI и зависимости не позднее чем через 4 часа от запуска плана.
2) Запустить контрольную группу из 50 пользователей.
3) При успешной проверке запустить 10% пользовательской нагрузки.
4) Через 15-30 минут проверить CPU, RAM, IOPS, задержки хранилища, ошибки подключения и время входа.
5) Последовательно увеличить нагрузку до 25%, 50%, 75% и 100%.

6) При достижении 6500 пользователей зафиксировать время восстановления и показатели производительности.

Контрольные показатели:

— пользователи проходят аутентификацию;
— пользователи получают назначенные BPM или приложения;
— среднее время подключения не превышает эксплуатационный норматив Заказчика;
— отсутствуют массовые ошибки брокера, Actor, гипервизора и транспортного шлюза;
— функционал UTAG доступен без деградации.

1.22 Журнал аварийного восстановления

При каждом запуске плана необходимо вести журнал.

Время	Действие	Ответственный	Результат	Примечание
	Зафиксирован инцидент			
	Принято решение о запуске DR			
	Проверены резервные копии			
	Восстановлены зависимости			
	Восстановлен сервер VDI			
	Восстановлены пулы и поставщики			
	Выполнена приемочная проверка			
	Сервис передан в эксплуатацию			

1.23 Регулярная проверка готовности

Для поддержания готовности плана необходимо:

— ежемесячно проверять успешность резервного копирования;
— ежеквартально выполнять тестовое восстановление сервера VDI и базы данных в изолированной среде;

— не реже одного раза в полгода выполнять учение по переключению на резервную площадку, если она предусмотрена архитектурой;
— после каждого обновления VDI проверять актуальность процедур восстановления;
— после изменения архитектуры обновлять схему зависимостей и целевые RTO/RPO;
— хранить актуальный комплект дистрибутивов, ключей, сертификатов и учетных данных в защищенном хранилище.

1.24 Критерии завершения аварийного восстановления

Аварийное восстановление считается завершенным, если:

— восстановлены все критические компоненты Системы;
— пользователи могут подключаться к назначенным BPM и приложениям;
— достигнут показатель восстановления 6500 пользователей за 8 часов или зафиксировано утвержденное отклонение;
— функционал платформы UTAG доступен без деградации;
— отсутствуют критические ошибки в журналах VDI, базы данных, гипервизора, Actor и транспортных шлюзов;
— администратор ИБ подтвердил отсутствие активной компрометации;
— руководитель восстановления передал Систему в штатную эксплуатацию.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

	Номера листов (страниц)				*Всего листов (страниц) в докум.*	*№ документа*	*Входящий номер доп. Документа и дата*	*Подп.*	*Дата*
Изм.	*изменен-ных*	*заменен-ных*	*новых*	*аннулиро-ванных*					