

Внутренний аудит удаленно - это реально?

**Колбаева Оксана
Александровна**

Старший консультант
Департамента внутреннего
аудита и управления рисками



Основные вопросы

- 1 Как организовать работу удаленно?
- 2 Актуализация плана работы аудиторов
- 3 На что обратить внимание в первую очередь?
- 4 Информационная безопасность и сохранность данных
- 5 Организация взаимодействия с другими подразделениями

Как организовать работу удаленно?

- Юридические и организационные аспекты;
- Рабочее место;
- Правильный настрой и распорядок дня:
 - планируйте,
 - восстанавливайтесь,
 - не работайте по ночам;
- Отвлекающие факторы;
- Ни дня без связи.



Как организовать работу удаленно?

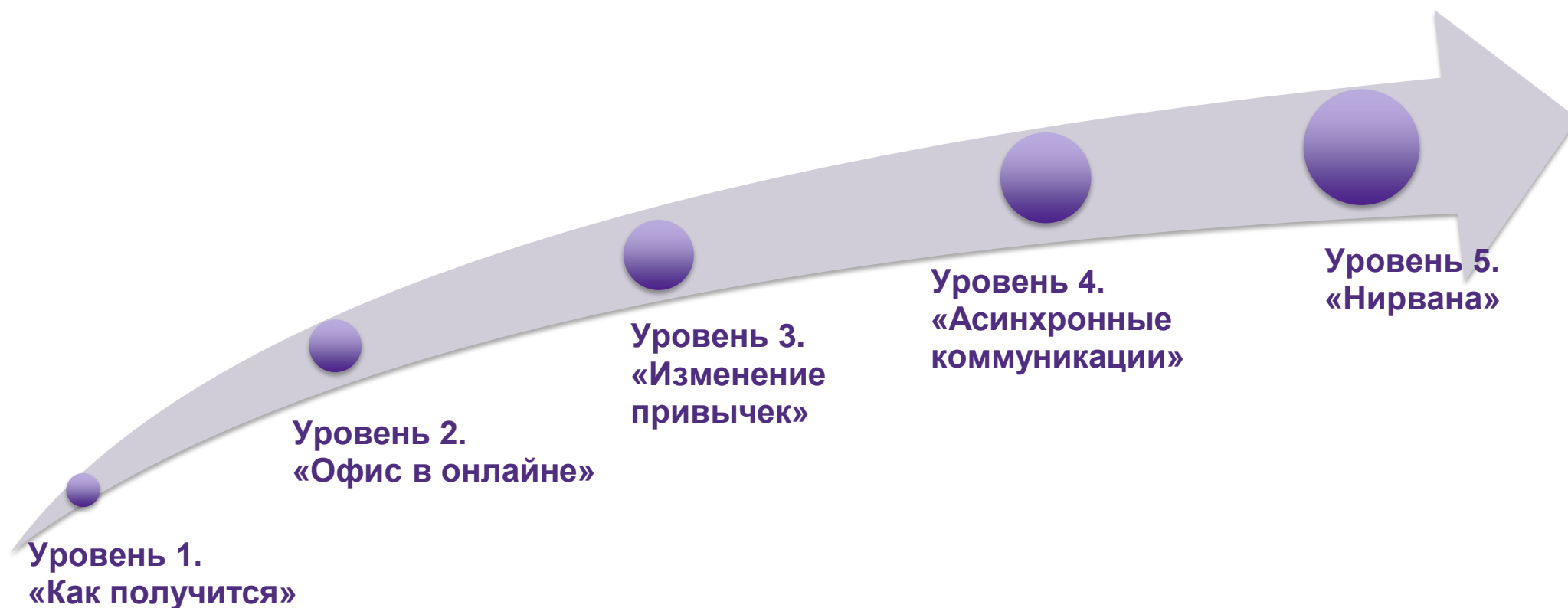
“

Как контролировать
присутствие
сотрудника на
месте?

”

Никак.
Контролируйте
выполнение задач.

Уровни организации удаленной работы*



* классификация предложена Мэттом Мулленвегом, основателем компании Automattic (создатель WordPress), где еще до коронавируса вообще не было единого офиса на 1170 сотрудников из 75 стран, говорящих на 93 языках.

“

Эпидемия закончится, а команда останется

”

Возможные ограничения

1. ограниченные возможности по проверке подлинности документов и представленных сведений;
2. ограниченность доступа к конфиденциальной информации;
3. сложности в установлении реальности существования активов;
4. проблемы коммуникации;
5. отсутствие соответствующих навыков у внутренних аудиторов;
6. увеличение нагрузки на проверяемое подразделение;
7. технологические ограничения.

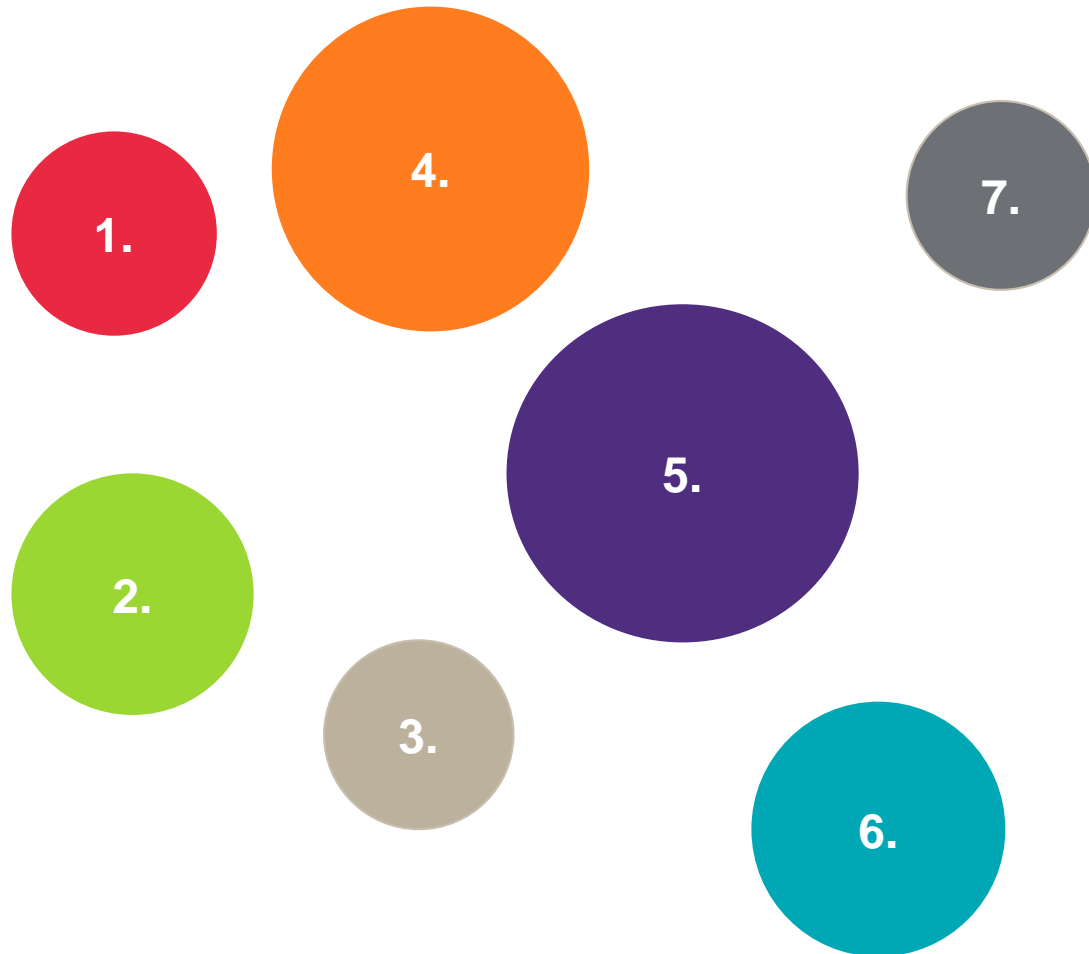
Актуализация плана работы аудиторов

- Оцените возможность дистанционного выполнения заданий с учетом:
 - их целесообразности в текущих условиях (в т.ч. с точки зрения затрат);
 - текущего и ожидаемого режима работы и возможности доступа к активам и персоналу;
 - качества данных и зрелости СУРиВК;
 - возможности перераспределения ресурсов внутреннего аудита;
 - ожидания заинтересованных сторон.
- В случае невозможности дистанционного выполнения заданий/отдельных работ в рамках задания:
 - оцените возможные последствия их невыполнения или несвоевременного выполнения;
 - проинформируйте об этом соответствующие заинтересованные стороны;
 - оцените возможность и целесообразность привлечения внешних поставщиков услуг.

Изменение аудиторских процедур

1. Проводите аудиторские процедуры, не требующие личного общения: сбор и анализ данных (за исключением личных интервью), написание отчетов, оформление рабочих документов.
2. Займитесь автоматизацией и стандартизацией внутренних процессов (обновите шаблоны рабочих документов, чек-листов и т.п. – всем тем, на что не хватало времени в работе).
3. По возможности замените все процедуры, требовавшие физического присутствия на объекте, на альтернативные, способные покрыть риски.
4. Организуйте онлайн-тренинги по повышению квалификации сотрудников внутреннего аудита.
5. Необходимо добавить аудиторские процедуры, позволяющие убедиться в непрерывности деятельности компаний.
6. Пересмотрите критерии оценки аудиторских доказательств (с точки зрения их достаточности, надежности, уместности и полезности)

Адаптация аудиторских процедур в условиях удаленной работы



Аудиторские процедуры:

1. Наблюдение
2. Выборочное тестирование (отслеживание и проверка документального подтверждения)
3. Пересчет
4. Интервью
5. Анализ и оценка данных
6. Инвентаризация
7. Подтверждения от третьих сторон

На что обратить внимание в первую очередь?

1. Наблюдение

1. Необходимо оценить имеющиеся компенсирующие средства контроля.
2. Использовать современные видеотехнологии.
3. При невозможности лично присутствовать на объекте аудита, руководитель может рассмотреть возможность компенсировать это путем:
 - привлечения внешнего консультанта;
 - привлечения независимых сотрудников из других департаментов

Проверка системы видеонаблюдения

1. Случались ли сбои работы камер? Как часто? Какие последствия сбоев?
2. Работают все камеры видеонаблюдения или только часть камер?
3. Куда направлены камеры видеонаблюдения? Что фиксируют камеры?
4. Какое разрешение у камер?
5. Где установлен сервер и накопители информации?
6. Кто отслеживает и снимает накопленную информацию?



На что обратить внимание в первую очередь?

2. Выборочное тестирование

1. Размер выборки может значительно увеличиться.
2. Необходимо пересмотреть подходы к оценке аудиторских доказательств с точки зрения их достаточности, надежности, уместности и полезности

На что обратить внимание в первую очередь?

3. Пересчет

Необходимо предусмотреть дополнительные процедуры для работы с конфиденциальной информацией

На что обратить внимание в первую очередь?

4. Интервью

1. Отсутствует возможность расположить к себе интервьюируемого.
2. Сложность оценки невербального общения.
3. При проведении личного интервью необходимо обеспечить безопасность интервьюируемого и внутренних аудиторов (социальная дистанция).
4. Запись только с разрешения интервьюируемого.

На что обратить внимание в первую очередь?

5. Анализ и оценка данных

1. Необходимо предусмотреть дополнительные процедуры для работы с конфиденциальной информацией.
2. Необходим навык работы внутренних аудиторов с большими объемами данными.
3. Дополнительная нагрузка на проверяемое подразделение

На что обратить внимание в первую очередь?

6. Инвентаризация

1. Отсутствие физического доступа к активам.
2. Рассмотреть возможность замены или компенсации процедуры (наблюдением или с использованием дронов).

На что обратить внимание в первую очередь?

7. Подтверждения от третьих сторон

1. Отсутствие доступа к конкретным контрагентам.
2. Необходимо договориться об использовании электронного документооборота с электронной подписью.

Информационная безопасность и сохранность данных

Риски при работе удаленно:

- Утечка конфиденциальной информации;
- Использование незащищенного подключения к сети;
- Проникновение вредоносного ПО на компьютер или в корпоративную сеть;
- Ненадлежащий контроль доступа;
- Раскрытие учетных записей и паролей;

Базовые рекомендации для безопасной работы удаленно

1. Не оставляйте устройства в свободном доступе;
2. Не подключайте к рабочему компьютеру чужие внешние носители и неизвестные мобильные устройства;
3. Установите пароль на домашнюю Wi-Fi сеть и не сообщайте его посторонним;
4. Старайтесь не использовать публичные точки доступа Wi-Fi и не используйте ноутбуки и мобильные устройства в публичных местах и в общественном транспорте (в т.ч. в поезде или самолете);
5. Используйте сложные пароли и периодически их меняйте;
6. Не открывайте файлы и не переходите по ссылкам, полученным от неизвестных лиц;
7. Включите автоблокировку устройств в случае отсутствия активности пользователя.

Корпоративные рекомендации для безопасной работы удаленно

1. Используйте только защищенный доступ к корпоративным ресурсам через VPN и многофакторную аутентификацию учетной записи;
2. Настройте и регулярно выполняйте резервное копирование данных с использованием корпоративной системы резервного копирования;
3. Не препятствуйте выполнению регулярных антивирусных проверок;
4. Регулярно перезагружайте компьютер, в т.ч. для обновления ПО;
5. Используйте только разрешенные в компании каналы передачи информации.

Рекомендации для безопасного использования портативных устройств

- Регулярно обновляйте систему;
- Используйте все предусмотренные возможности для разблокировки устройства;
- Устанавливайте приложения только из официальных источников;
- Не храните на мобильных устройствах или в персональных облачных сервисах рабочие документы;
- Включите автоблокировку мобильного устройства;
- Используйте службы Apple и Google, позволяющие удалять информацию в случае утери портативного устройства;
- Не используйте мессенджеры и публичные почтовые сервисы для пересылки незашифрованных рабочих документов;
- Включите двухшаговую проверку в мессенджерах.

Организация взаимодействия с другими подразделениями

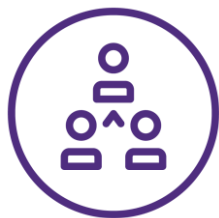
- Разработать и внедрить системный подход к коммуникациям;
- Использовать различные способы взаимодействия с подразделениями;
- Обеспечить внутренним аудиторам прямой доступ к сотрудникам (в т.ч. к руководству)
- Выявить и устранить возможные проблемы в части доступа внутренних аудиторов к необходимой информации;
- Организовать безопасное хранилище данных для информационного обмена.

“

**Переход на удаленный режим – это
возможность протестировать новый
формат работы**

”

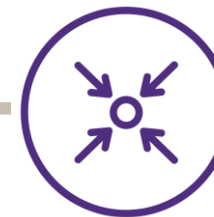
Наши услуги



**Аутсорсинг / косорсинг
внутреннего аудита**



**Совершенствование
функции внутреннего
аудита**



**Внешняя оценка качества
функции внутреннего
аудита**



**Актуализация/разработка
плана ОНиВД**



**Обучение внутренних
аудиторов**



**Проверки на соответствие
требованиям**

Наши услуги



**Диагностика рисков
проектов и организаций**



**Оценка зрелости систем
управления рисками и
внутреннего контроля**



**Совершенствование
СУР и СВК**



**Оценка и разработка
моделей оценки рисков**



**Оценка системы
внутреннего контроля в
рамках внешних аудитов**



**Поддержка налогового
мониторинга**

Контакты



Оксана Колбаева

*Департамент внутреннего аудита и управления рисками,
аккредитованный преподаватель Института
Профессиональных Бухгалтеров России*

T +7 (495) 737 5353 [доб. 5503]

E KolbaevaO@fbk.ru



Роман Кенигсберг

Директор

Департамент внутреннего аудита и управления рисками

T +7 (495) 737 5353 [доб. 4555]

E KenigsbergR@fbk.ru

Благодарим за внимание!

101990, Москва,
ул. Мясницкая, 44/1, стр.2АБ
Телефон (495) 737 5353
Факс (495) 737 5347
E-mail fbk@fbk.ru

