

Особенности работы распределенных команд в ИБ: опыт заказчика

**Константин
Саматов**

Член Правления Ассоциации
руководителей служб
информационной безопасности





1

Преимущества и недостатки удаленной работы



2

Как повысить эффективность удаленных сотрудников?



3

Требования по защите информации при обеспечении безопасной дистанционной работы



Дисклеймер: исключительно на опыте работы в сфере ИБ

1

Преимущества и недостатки удаленной работы



ПРЕИМУЩЕСТВА УДАЛЕННОЙ РАБОТЫ

- **Глобальный доступ к талантам:** возможность найма специалистов в любой точке мира страны
- **Повышение продуктивности:** устранение временных затрат на поездки и создание комфортных условий для работы
- **Снижение затрат на офис:** экономия на аренде помещений и обслуживании офисной инфраструктуры
- **Гибкий график и удовлетворенность сотрудников:** улучшение баланса между работой и личной жизнью, что влияет на мотивацию, а также на зарплатные ожидания

1

Преимущества и недостатки удаленной работы

ОГРАНИЧЕНИЯ И ПОТЕНЦИАЛЬНЫЕ ПРОБЛЕМЫ

- **Ограниченная коммуникация:** возможные сложности в коммуникации и взаимодействии
- **Недостаток контроля:** затруднен мониторинг рабочего процесса и производительности
- **Проблемы с безопасностью данных:** риск утечек и несанкционированного доступа к конфиденциальной информации
- **Сложности в адаптации новых работников:** сложности в формировании общего понимания и ценностей компании



2 Как повысить эффективность удаленных сотрудников?

ФАКТОРЫ ЭФФЕКТИВНОСТИ В УСЛОВИЯХ УДАЛЕННОЙ РАБОТЫ

- **Технологическая инфраструктура:** инструменты для удаленной работы, включая высокоскоростной интернет и безопасное программное обеспечение
- **Коммуникации:** средства онлайн-коммуникации и проектного управления для обеспечения эффективной коммуникации и совместной работы.
- **Гибкий подход:** гибкие методы управления временем и задачами, чтобы соответствовать потребностям разнообразной географически распределенной команды, четкие цели и системы измерения производительности для учета результативности удаленной работы.
- **Обучение и развитие:** возможности для обучения и развития, чтобы сотрудники были в курсе последних технологий и методов работы.



2 Как повысить эффективность удаленных сотрудников?

ОПТИМАЛЬНЫЙ НАБОР ТЕХНОЛОГИЙ ДЛЯ ОПЕРАТИВНОГО НАЛАЖИВАНИЯ УДАЛЕННОЙ РАБОТЫ

- 1. Видео-конференции:** коммуникации, визуальное взаимодействие.
- 2. Проектное Управление:** организация задач, совместная работа.
- 3. Облачные Хранилища:** общий доступ к файлам, гибкий и безопасный доступ («свои» облачные хранилища).
- 4. Сервисы оперативной коммуникации:** мгновенное общение, обмен информацией.
- 5. Виртуальные рабочие столы:** доступ к рабочему пространству из любого места.
- 6. Коллективное редактирование:** совместное редактирование документов.
- 7. Безопасность и Аутентификация:** VPN, двухфакторная аутентификация.



2 Как повысить эффективность удаленных сотрудников?

ОНБОРДИНГ НОВИЧКОВ-УДАЛЕНЩИКОВ В КРОСС-КОМАНДНЫЕ ПРОЦЕССЫ И ПРОЕКТЫ

Онбординг – это процесс интеграции новых сотрудников в компанию. Он включает в себя знакомство с коллегами, корпоративной культурой и основными процессами компании.

Этапы:

Первый этап – знакомство с компанией и ее процессами: **welcome** – встреча, адаптационный чеклист, обучающий курс и/или путеводитель

Второй этап – техническая интеграция: изучение основных инструментов, используемых в работе, обучение правилам безопасности и рассмотрение конкретных кейсов из практики компании

Третий этап – наставничество и поддержка со стороны опытных коллег

Четвертый этап – оценка процесса и обратная связь



3 Требования по защите информации при обеспечении безопасной дистанционной работы

Отдельный АРМ (ноутбук)

Обязательно оборудование отдельным техническим средством

Защита рабочего места

Установленный корпоративный софт с соответствующими настройками безопасности

Шифрование мобильного устройства

Если АРМ используется для командировок обязательно шифрование имеющейся на нем информации

Обучение сотрудников

Обучение базовым принципам безопасности. Проведение мероприятий по предотвращению социальной инженерии и фишинговых атак



Спасибо!

Константин Саматов

Член Правления Ассоциации руководителей служб
информационной безопасности

