

**Сотрудники снова в офисе. Выводы,
которые нужно сделать для эффективной
борьбы с утечками или
не DLP единой**

АО ВТБ Специализированный депозитарий

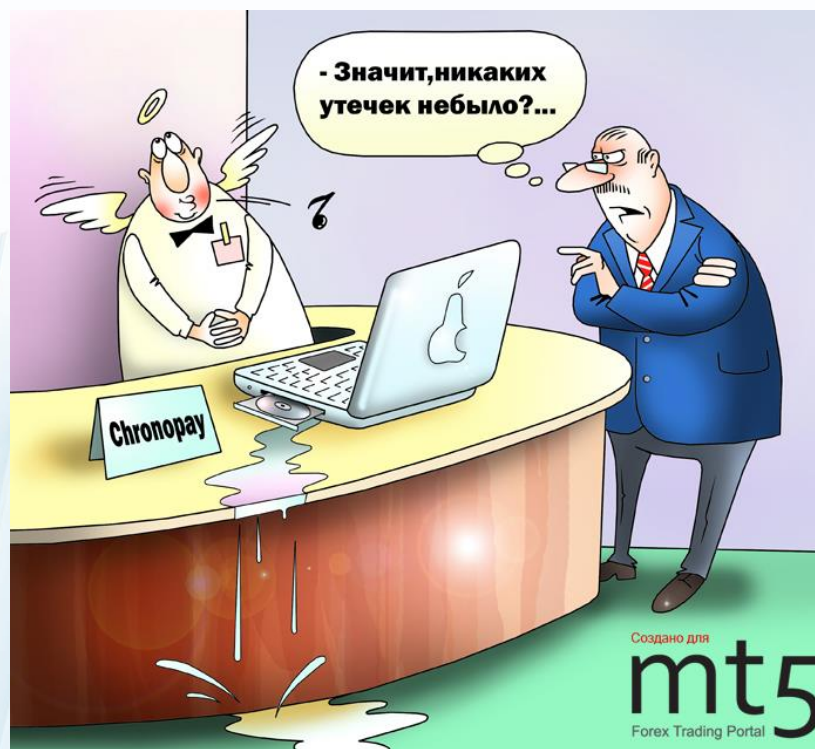
Переходим на удаленную работу



Основные подготовительные мероприятия для организации удаленной работы

АО ВТБ Специализированный депозитарий

Что нужно сделать для эффективной и безопасно удаленки



Необходимо понять и принять, что 100 % гарантии от утечки информации - нет

Удаленный формат работы повышает вероятность утечки защищаемой информации в разы

АО ВТБ Специализированный депозитарий

На первое место выходит доверие к сотрудникам Компании



Так как осуществлять контроль за соблюдением сотрудниками конфиденциальности при удаленной работе крайне проблематично

АО ВТБ Специализированный депозитарий

Знай, к каким ресурсам сотруднику предоставляется доступ при удаленной работе

Уровень конфиденциальности и критичности ресурсов

Возможные каналы утечки информации (модель угроз)

Вероятность утечки данных и способы их предотвращения

Возможные последствия при утечки данных



Оценка рисков и принятие решения – бизнес (руководство)

АО ВТБ Специализированный депозитарий

Как предотвращать утечку конфиденциальной информации

Не DLP единой

Data Loss Prevention



АО ВТБ Специализированный депозитарий

Проведение разъяснительной работы и обучение персонала



Дополнительное доведение инструкций, порядков, правил (под подпись)

Предусмотреть порядок юридически-значимого доведения вновь разработанных ОРД до сотрудников

Довести порядок осуществления контроля, а также чем а также чем данный контроль регламентируется

АО ВТБ Специализированный депозитарий

Обеспечение безопасного удаленного подключения к информационным системам
Компании

Создание защищенных каналов связи

Реализация двухфакторной аутентификации

Организация терминального доступа к информационным системам Компании

Определение информационных ресурсов Компании
к которым предоставляется удаленный доступ

Технология предоставления удаленного доступа

Закрытие/контроль буфера обмена

Агент DLP на терминале/рабочих станциях

АО ВТБ Специализированный депозитарий

Неожиданный успех в использовании DLP

Использование практически всех возможностей по контролю за эффективностью сотрудников Компании



АО ВТБ Специализированный депозитарий

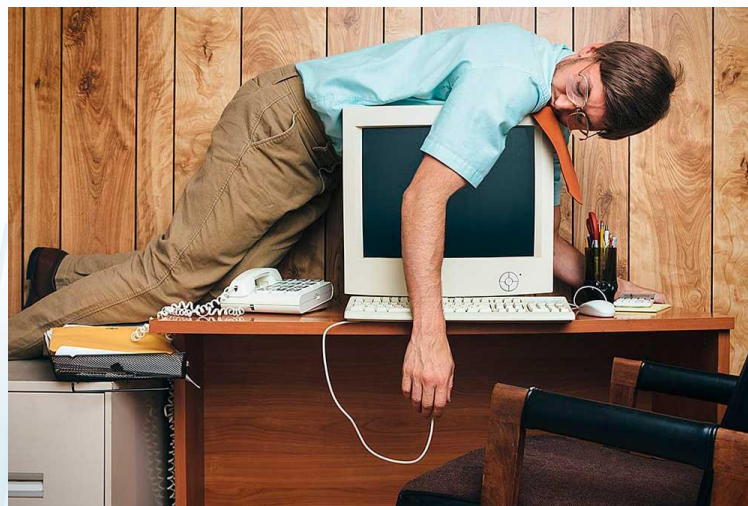
И все таки они вернулись....сотрудники



Какие угрозы?

АО ВТБ Специализированный депозитарий

Расслабленность сотрудников



Необходимо

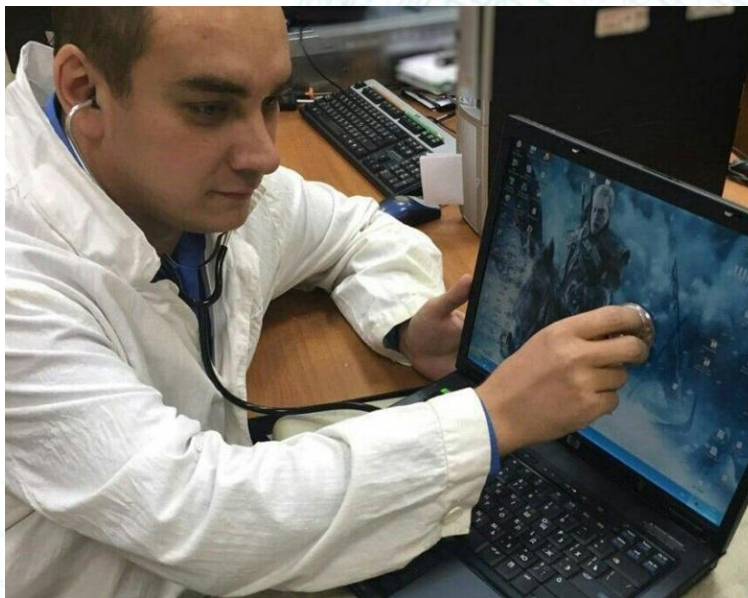
Проведение дополнительных инструктажей (дополнительно, вживую)

Доведение до сотрудников под подпись новых ОРД по ИБ

Получение уточняющей информации в отношении возможных изменений в бизнес процессах

АО ВТБ Специализированный депозитарий

Возврат выданных ПК



Машины, долгое время не подключающиеся к корпоративной сети, действительно могут нести угрозу вирусного заражения

АО ВТБ Специализированный депозитарий

Использование DLP в процессе работы с информацией

Варианты использования	Что ищем/защищаем	Чего достигаем (каков эффект)
Поиск информации в локальных/закрытых ИС	Информацию, которая потенциально может быть отнесена к ГТ	Снижаем риск наступления уголовной ответственности, снижение репутационного ущерба
Противодействие утечки информации	Информация составляющая КТ, РИД	Предотвращение экономического ущерба в размере упущенной выгоды, в случае разглашения возможность взыскания /компенсации в судебном порядке
	Персональные данные сотрудников/клиентов	Предотвращение экономического ущерба в сумме возможного наложенного штрафа, компенсации за моральный ущерб в судебном порядке. Предотвращение репутационного риска связанного с уходом клиентов (упущенная выручка), не приходом новых клиентов
	Конфиденциальная информация	Возможность применение дисциплинарной ответственности к нарушителям, снижение репутационного риска
	Аутентификационная информация (логин пароль)	Позволило своевременно предотвратить НСД к критически важным ИС в целях их компрометации и вывода из строя
	Информация о выпущенных кредитных картах	Предотвращение судебных исков, экономического ущерба, защита ПДн

АО ВТБ Специализированный депозитарий

Использование DLP в процессе работы с сотрудниками

В процессе анализа информации	
Выявляемые признаки	Эффект
Выявление лиц из групп риска: - азартные игры; - алкоголь, наркотики; - долги, кредиты; - крупные покупки.	Возможность предотвращения экономического и репутационного ущерба в виду попадания сотрудника в зону риска, возможность свершения противоправных действий направленных на извлечение незаконной выгоды, деструктивное воздействие на коллектив, снижение качества выполняемой работы, возможность ухода/недовольства клиентов. Возможное свершение противоправных действий: сопоставление значимых покупок и реальных доходов. Финансовые затраты на локализацию негативных последствий.
Выявление лиц стремящихся сменить работу	Внезапное увольнение сотрудников может привести к незапланированным затратам по: - поиску нового сотрудника; - Обучению и вводу в коллектив нового сотрудника; Невыполнение обязанностей по должности до ввода сотрудника в должность. Возрастание нагрузок на остальных сотрудников.

АО ВТБ Специализированный депозитарий

В процессе анализа перехватываемой информации

Выявляемые признаки	Эффект
Выявление неформальных деструктивных лидеров:	Внесение разобщенности и смуты в коллектив. Срыв выполнения поставленных задач. Сопротивление инновациям. Экономический ущерб от деструктивной деятельности.
Выявление неформальных лидеров:	Использование для выполнения поставленных задач, вовлечение сотрудников и т.д.

В процессе использования дополнительных функций

Анализируемая информация	Эффект
Активность пользователей	Рациональное и качественное использование рабочего времени (актуально на удаленке), оптимальное задействование сотрудников, перераспределение обязанностей
Табель учета рабочего времени	
Активность процессов	
Эффективность работы сотрудников	

Спасибо за внимание

Луганцев А.А.
15.04.2022