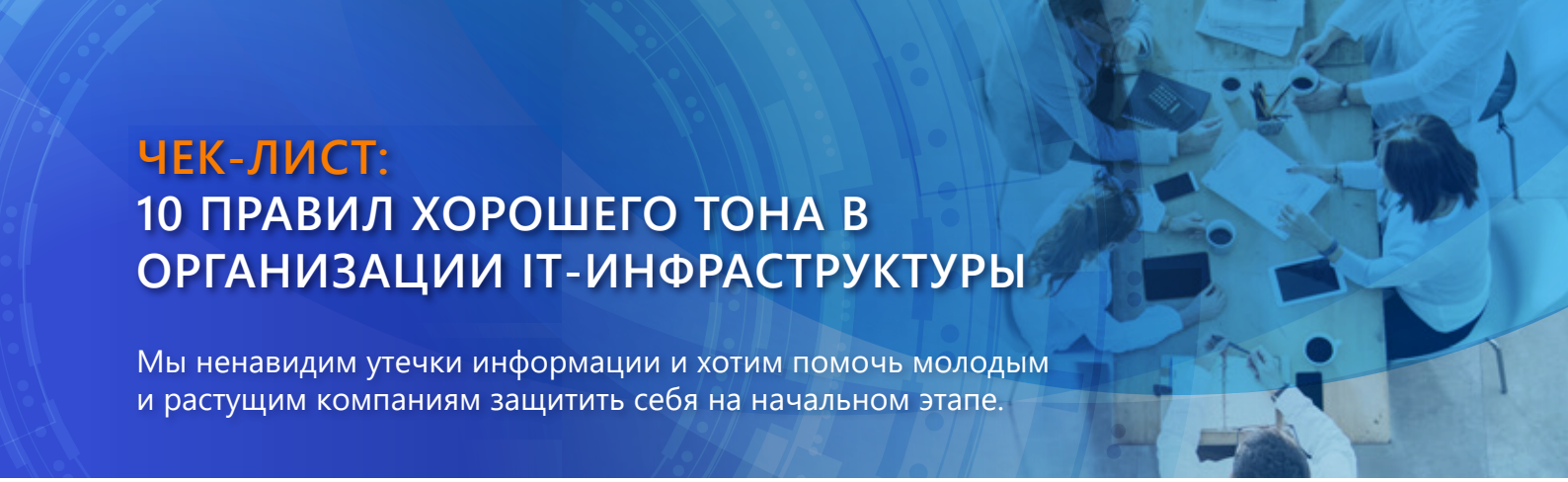

ЧЕК-ЛИСТ:
10 ПРАВИЛ ХОРОШЕГО ТОНА В ОРГАНИЗАЦИИ IT-ИНФРАСТРУКТУРЫ

Мы ненавидим утечки информации и хотим помочь молодым и растущим компаниям защитить себя на начальном этапе.

Вот необходимый минимум с точки зрения информационной безопасности:

1. Программное обеспечение.

Определите жизненно важный минимум ПО для обеспечения бизнес-процессов компании. Используйте только лицензионный либо свободно распространяемый софт от надежных поставщиков и регулярно его обновляйте.

2. Антивирусная защита.

Если нет средств на покупку лицензий от хорошего вендора, регулярно обновляйте Windows и не отключайте стандартный защитник. Не забывайте и о компьютерах на Linux и OSX – они, хоть и в меньшей степени, но тоже подвержены атакам.

3. Роутеры, коммутаторы, принтеры, Wi-Fi.

Сразу же уберите стандартный пароль на всех маршрутизаторах, коммутаторах, мини-АТС, принтерах и создайте изолированную гостевую сеть Wi-Fi (только Интернет, без возможности подключиться к локальной сети) и отдельный Wi-Fi для сотрудников.

4. Данные.

Разделяйте данные по категориям (секретные, конфиденциальные, важные, бухгалтерия и т.д.) и храните их в определенных местах – сетевых папках или сетевых хранилищах с разграниченными по пользователям правами доступа.

5. Шифрование жесткого диска.

Включите стандартный Windows Bitlocker и зашифруйте важные папки или весь диск на тех рабочих станциях, где есть ценные данные. Установите и сохраните пароль от Bitlocker на флешку или запишите на листок, запечатайте и отдайте директору или специалисту по безопасности.

6. Корпоративная почта.

Используйте корпоративный почтовый сервис, например, от Google, если нет средств и специалистов развернуть свой почтовый сервер. Ваши личные почтовые ящики могут быть уже давно украдены, просто вы не знаете об этом. Кстати, тут можно это узнать.

7. Резервное копирование.

Регулярно производите резервное копирование. Желательно настроить правила копирования по расписанию. Один бэкап в день – хорошая практика.

8. Двухфакторная аутентификация для важных служб.

Настройте двухфакторную авторизацию для доступа к критичным для компании службам и сервисам, доступным извне.

9. Шифрование.

Используйте только зашифрованные каналы передачи данных: https, ftps, vpn-соединения между офисами и для доступа в локальную сеть компании извне.

10. Ликбез среди сотрудников.

Возможно, это самый важный пункт в списке. Регулярно проводите тренинги и объясняйте сотрудникам важность сложных паролей, блокировки сеанса рабочего стола, расскажите (а лучше покажите) что такое фишинг, и почему нельзя сразу открывать ссылки в письмах и сообщениях. Вот полезная статья о том, как лучше всего это делать.

SEARCHINFORM
INFORMATION SECURITY