

*Data
Protection is
People
Protection*



РУКОВОДСТВО ПО ЗАЩИТЕ ДАННЫХ И КОНФИДЕНЦИАЛЬНОСТИ:

Шифрование файла

В этом разделе рассматривается базовый пример шифрования файла с помощью функции Microsoft, доступной на компьютерах Mercy Corps. Существует ряд факторов, которые следует учитывать при шифровании файла, но конкретно здесь мы сосредоточимся на использовании пароля и шифровании одного файла. См. приведенные ниже ссылки на ресурсы, которые более подробно раскрывают суть шифрования. Однако для этого руководства полезно понимать тонкую разницу между «защитой паролем» и «шифрованием».

Думайте о защите паролем как о коробке с замком. Когда вы «защищаете паролем» свой документ, вы кладете его в электронный ящик и запираете его паролем: только тот, у кого есть пароль, может открыть ящик. Однако, если выбранный вами пароль не очень надежный или если он предоставлен не тому человеку, кто-то может легко получить доступ к ящику и просмотреть ваш документ! Шифрование же, напротив, использует сложные алгоритмы для кодирования информации, что требует наличия ключа для расшифровки этой информации. Представляйте это так, как будто вы берете свой документ и пропускаете его через машину для измельчения бумаги, в которой есть специальная клавиша, чтобы воссоздать документ.

Когда вы сочетаете защиту паролем и шифрование, вы фактически удваиваете свою защиту. Если кто-то успешно взломает пароль к электронному ящику, он сможет увидеть только «кусочки измельченной бумаги», не имея при этом надлежащего ключа. Все ноутбуки Mercy Corps зашифрованы с помощью Microsoft BitLocker. Это предотвращает извлечение жесткого диска ноутбука Mercy Corps и доступ к нему на другом компьютере.

☆ Важность

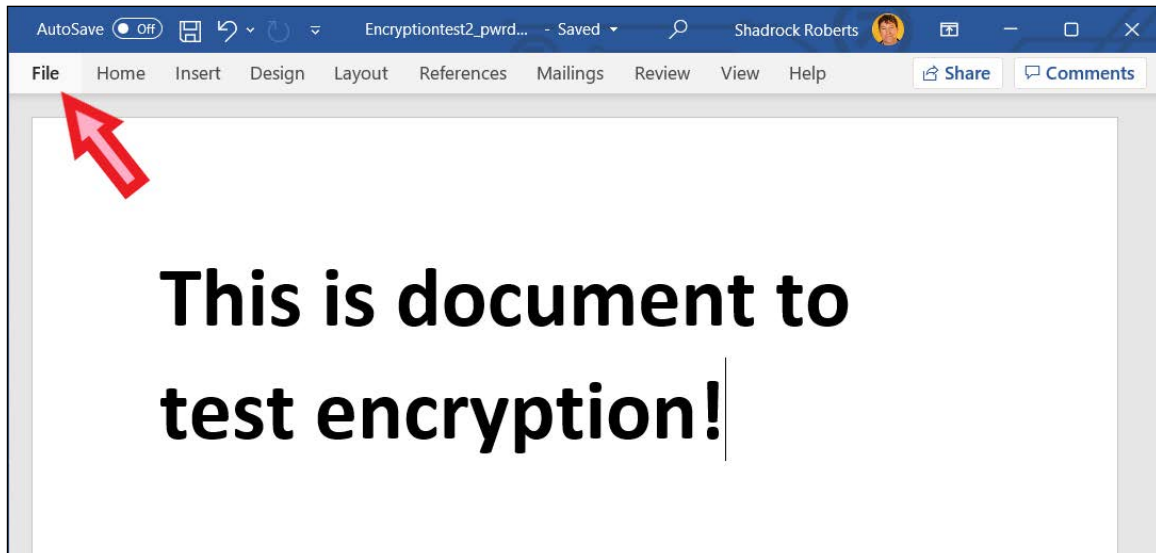
Шифрование имеет решающее значение, поскольку оно помогает обеспечить конфиденциальность и безопасность информации. Без шифрования данные могут быть перехвачены и прочитаны любым, кто имеет к ним доступ. Рассматривая вопрос о том, следует ли шифровать данные, спросите себя: «Каков риск для участников, сотрудников и партнеров программы Mercy Corps, если эти данные будут утеряны или украдены?» Хорошее проверенное правило — шифровать все, что содержит личную или закрытую («чувствительную») информацию.

📄 Принципы

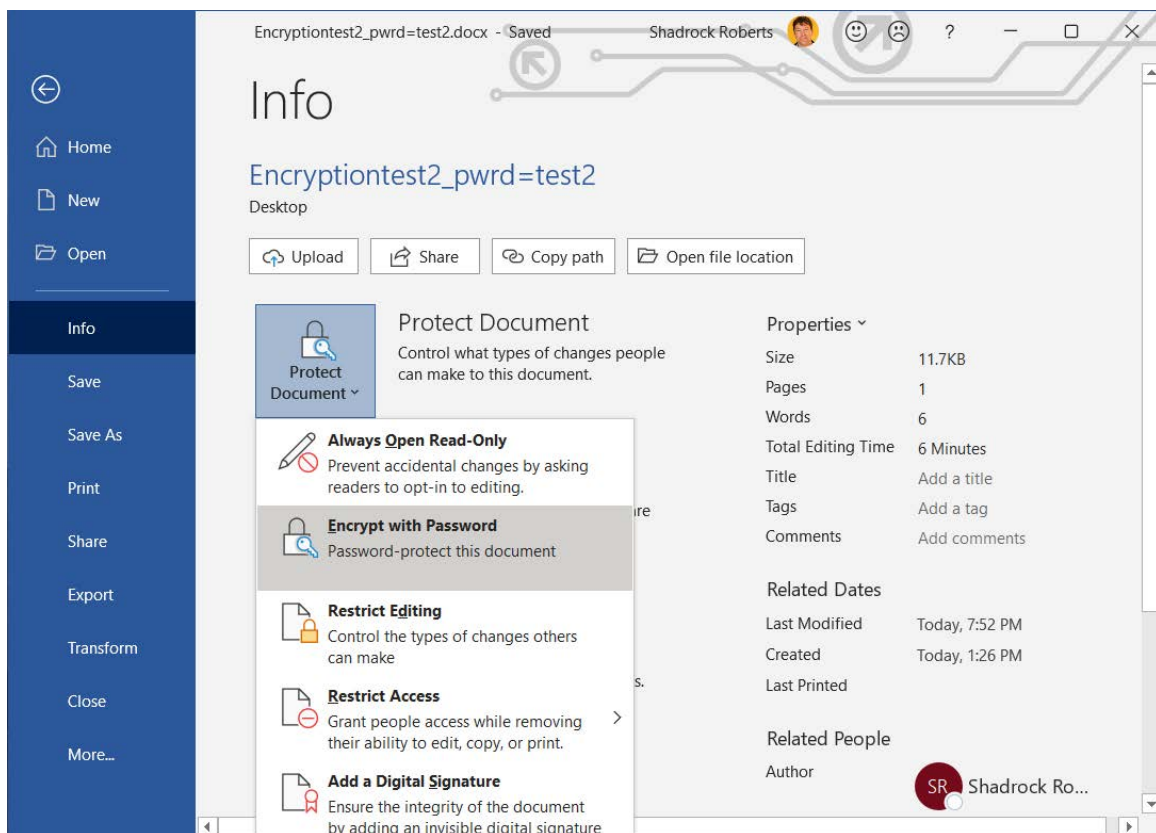
- › Используйте одобренные Mercy Corps системы для зашифрованной передачи и хранения данных (например, Microsoft SharePoint или Google Drive). Если вы сомневаетесь, обратитесь за советом к местному IT-специалисту.
- › Шифруйте конфиденциальные данные на всех этапах их сбора, использования, передачи и хранения.
- › Используйте надежные пароли и не используйте их повторно. Списки паролей распространяются в Интернете и упрощают доступ к нескольким вашим учетным записям или файлам для тех, у кого есть один из ваших паролей! Вы можете использовать менеджер паролей, например Lastpass. Однако менеджеры паролей могут быть уязвимы для кибератак со стороны поддельных приложений, поэтому крайне важно, чтобы менеджеры паролей использовались как часть более широкого подхода к защите данных.
- › Однако, для шифрования в командной среде не следует забывать о принципе «где тонко, там и рвется». Если хотя бы один человек не использует шифрование, данные вашей программы находятся под угрозой. Чрезвычайно важно сообщить об этом вашей команде: шифрование — это не только вопрос технологии, но и корректировки поведения.
- › Изучите законы, регулирующие шифрование в вашей стране. Местные законы в ряде стран (например, в Судане, Йемене и Пакистане) накладывают ограничения на программное обеспечение для шифрования. Если вы сомневаетесь, обратитесь за советом к местному IT-специалисту: как правило, они помогают вам обеспечить надлежащее шифрование жесткого диска вашего компьютера с помощью Intune.

Инструкции

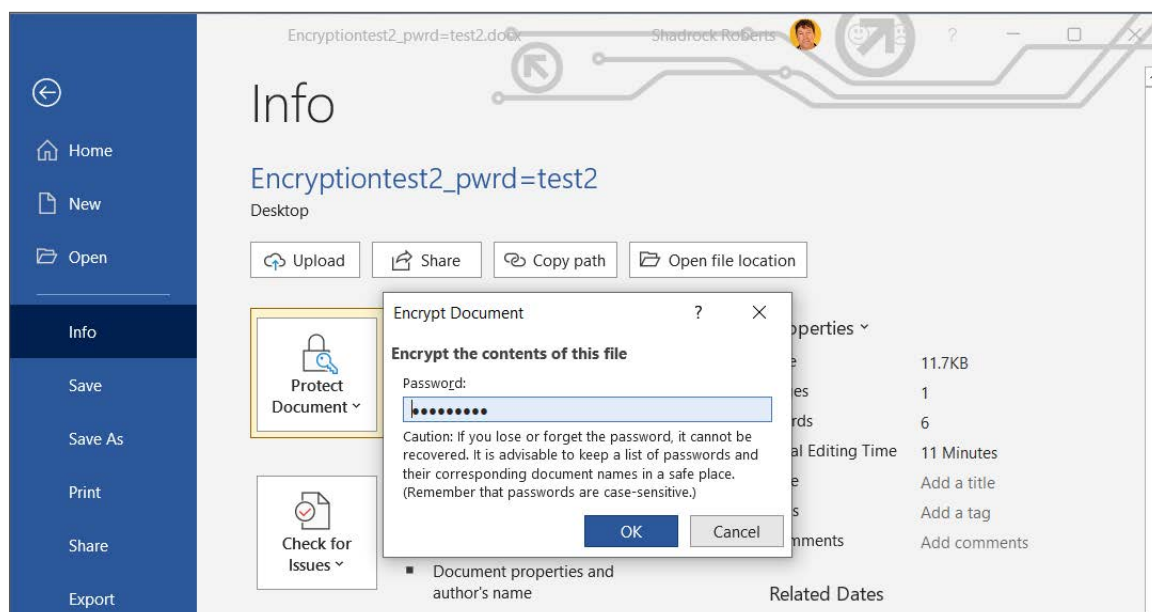
1 Откройте файл Word, Excel или PowerPoint, который нужно зашифровать, и выберите меню **Файл**.



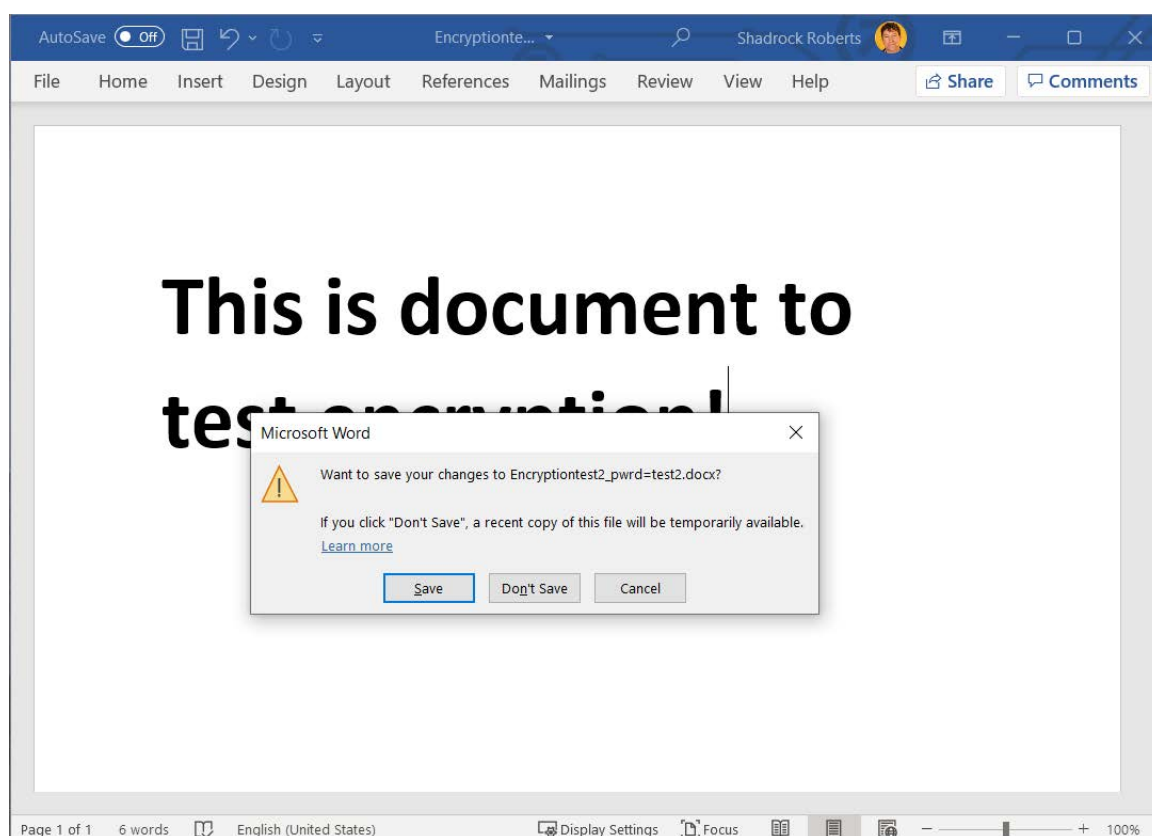
2 Перейдите к **Информация > Защитить документ > Зашифровать паролем**.



3 Введите пароль, нажмите **ОК**, затем введите его еще раз для подтверждения.



4 Сохраните файл для вступления пароля в силу.



Теперь вы можете поделиться файлом и паролем с теми, кому требуется доступ. Рекомендуется поместить файл в одобренную Mercy Corps облачную службу, такую как G Suite или SharePoint. Не забудьте отправить ссылку на файл и ссылку на пароль отдельно. Например, вы можете поделиться файлом с помощью Google Диска (Google Drive) (**См. раздел «Совместный доступ к файлам»**) и создать уведомление о том, что файл был предоставлен через Google, а затем передать пароль по электронной почте коллеге.

Дальнейшая помощь

- › [Стартовый комплект данных](#) от Electronic Cash Transfer Learning Action Network содержит список подсказок по шифрованию (см. список подсказок № 5).
- › Electronic Frontier Foundation предоставляет более [подробный обзор различных форм шифрования](#).
- › [Справочник современного специалиста в области развития](#) от Engine Room, включает раздел об управлении данными, в котором приводятся дополнительные общие сведения о шифровании.

КОНТАКТЫ

ХИЗЕР ЛАВ (HEATHER LOVE)

Директор по глобальной защите данных и конфиденциальности | IT
hlove@mercycorps.org

ШЕДРОК РОБЕРТС (SHADROCK ROBERTS)

Специалист по защите данных | IT
shroberts@mercycorps.org

О Mercy Corps

Mercy Corps — ведущая международная организация, в основе работы которой лежит вера в возможность сделать этот мир лучше. В бедствиях и в трудностях, в более чем 40 странах мира мы трудимся, чтобы претворять в жизнь смелые решения, помогая людям преодолевать невзгоды и строить более сильные изнутри сообщества. Сейчас и для будущего.



Международная штаб-квартира

45 SW Ankeny Street
Portland, Oregon 97204
888 842 0842
mercycorps.org

Европейская штаб-квартира

40 Sciences
Edinburgh EH9 1NJ
Scotland, UK
+44 131 662 5160
mercycorps.org.uk