



# Анонимность e-mail

Алексей Августинovich, [webhome.by](http://webhome.by)

# Лицензия

---

- ▣ **Выражаю согласие на обнародование представленного материала на принципах лицензии GNU Свободной Документации подготовленной мной публикации**



# Новый электронный адрес

---

- ▣ 1. Заведите **секретный e-mail**, старый может быть «засвечен»
- ▣ 2. Рекомендуется [gmail.com](https://gmail.com)
- ▣ 3. Используйте **шифрование данных** «<https://..>» [1]



# Правила регистрации секретной почты

---

- ❑ 1. Указывайте при регистрации **псевдоним**
- ❑ 2. Не привязывайте **номер телефона** к своим аккаунтам.
- ❑ 3. Не используйте **секретные вопросы**.
- ❑ 4. Не привязывайте разные **аккаунты друг к другу** (особенно фейсбук к почте). [2]



# Настройки браузера

---

- **Перед регистрацией нового адреса «почистите кеш»**

(Как это сделать спросите у гугла)

- **Максимально используйте режим инкогнито в браузере.**
- **Перехват cookie один из самых распространённых способов угона доступа. В режиме инкогнито все новые cookie автоматически удаляются после закрытия окна. [2]**



# Выбор пароля

---

- Большие и маленькие буквы, спецсимволы
- Более 8 символов
- Уникальный пароль для каждого сервиса – идеально
- Несколько паролей для сервисов разного уровня – реально
- Придумайте мнемонический алгоритм для создания своих паролей.



# Ошибки при выборе пароля

---

- Даты
- Дни рождения
- Фамилии
- Имена
- Клички
- qwerty и т.п.
- Цифровые пароли



# Уязвимости паролей

---

1. Простой пароль
2. Ответ на «вопрос безопасности» - легко узнать!
3. Повтор паролей для разных аккаунтов
4. Сканирование клавиатуры в Интернет-кафе.
5. Кража cookie-файла
6. Перехват информации в онлайн
7. Перехват SMS для восстановления пароля
8. Утрата устройства с залогиненными сервисами  
**(ВСЕГДА нажимайте «ВЫХОД»!) [3]**





# Хранение паролей

---

- Программа для локального хранения KeePass.info
  - Открытие мастер-паролем
  - Опция – наличие файла-ключа на флешке
- Сервис запоминания паролей lastpass.com – хранит информацию на сервере и локально на устройстве
  - Действует через плагины для браузера. Есть локальная утилита для просмотра паролей и записей. [3]



# БОНУС! Шифрование почты

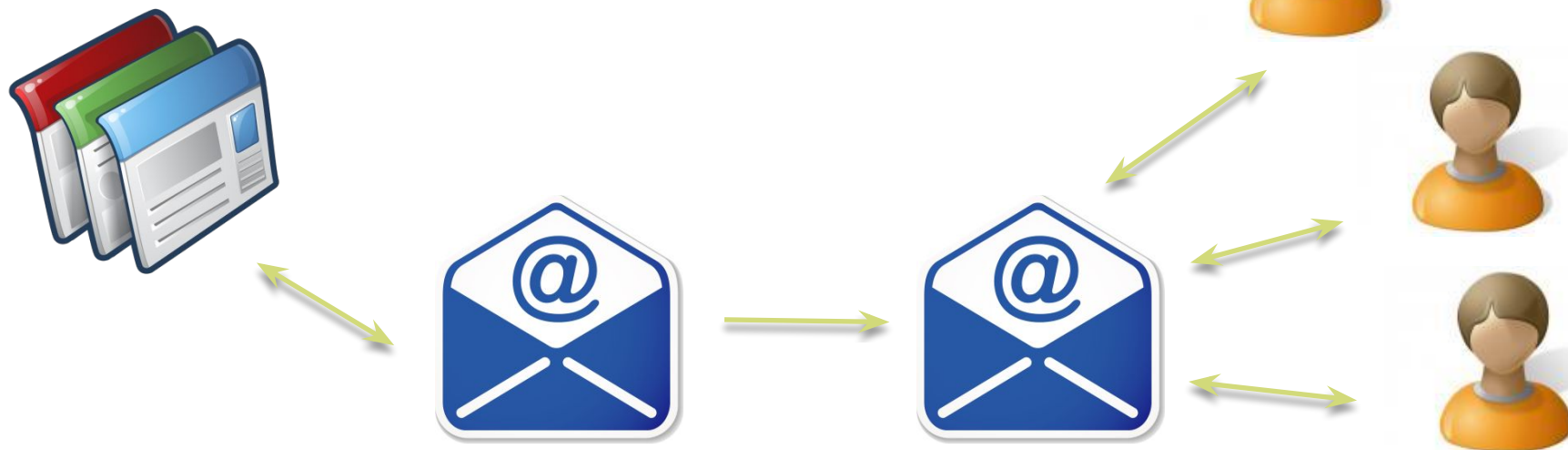
---

- Система создания двойных ключей: личный и публичный. Для почты и прочих данных:
- [www.gnupg.org](http://www.gnupg.org)
- Отправитель и получатель должны создать свои пары ключей и обменяться публичными ключами. [3]



# Схема шифрования почты

---



**Секретный - для сервисов**  
**secretmail@example.com**

**Основной - для людей**  
**myname@domain.com**



# Анонимный прокси-сервер

---

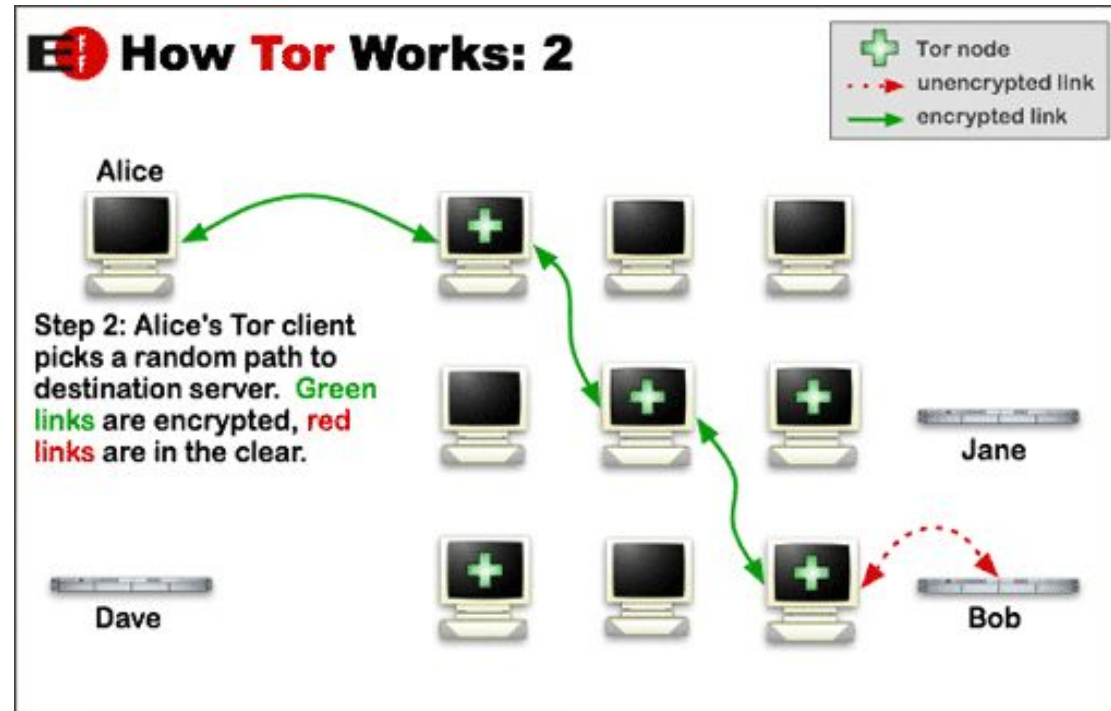
- Если работаете со своего домашнего ПК, то лучше использовать **анонимный прокси-сервер**.
- Найти:
  - Список бесплатных прокси-серверов можно найти, например, по адресу [publicproxyservers.com](http://publicproxyservers.com).
  - Вбить в поисковой строке Google фразу "proxy server high anonymity".

Минус – замедляет скорость.



# Анонимное сетевое соединение

- Если есть возможность – установите программу TOR
- Скачать по адресу [torproject.org](http://torproject.org)
- TOR также предлагает "мобильную" версию - Xero Bank Browser [1]



# Шифрование и анонимность

---

- Браузер на основе Firefox:
  - Не ставить плагины
  - Не открывать файлы из интернета (могут обращаться в сеть)
- [tails.boum.org](https://tails.boum.org) – операционная система на флешке, которая использует Tor [3]



# БОНУС . Заведите VPN за границей.

- Платная услуга:
- [cyberghostvpn.com](http://cyberghostvpn.com)
- [perfect-privacy.com](http://perfect-privacy.com)
- [www.swissVPN.net](http://www.swissVPN.net)
- [www.strongvpn.com](http://www.strongvpn.com)

[3]

VPN в интернете



# Использованные и рекомендуемые материалы

---

- 1. Анонимно в сети: как уберечься от интернет-слежки? [bit.ly/TSI rz4](http://bit.ly/TSI rz4)
- 2. Правила онлайн-безопасности: [bit.ly/QfxCpF](http://bit.ly/QfxCpF)
- 3. Материалы VuHub [bit.ly/QXgZAX](http://bit.ly/QXgZAX)
- 4. Как быть анонимным, PDF (англ): [bit.ly/SKucyj](http://bit.ly/SKucyj)
- 5. Анонимность в интернете [bit.ly/OuooXT](http://bit.ly/OuooXT)
- Защита конфиденциальных данных и анонимность в интернете [bit.ly/US3LUJ](http://bit.ly/US3LUJ)

