Цифрова безпека для журналістів

Чим ми ризикуємо?

- **Фактори ризику в разі несанкціонованого доступу**
  - Список контактів
  - Список дзвінків
  - Історія браузера
  - Листування по електронній пошті
  - Дані (фото, відео, документи)
  - Переговори (голос, чат)
  - Облікові записи
  - Банківські дані

Про що будемо говорити?

- Захист телефону
- Захист комп'ютера
- Захист облікових записів
- Захист даних
- Захист голосової і мережевої комунікації

Смартфон

Захист телефону

- Вибрати надійний пароль
- Включити шифрування
- Включити автоблокування екрану
- Користуватися безпечними мессенджерами
- Не встановлювати сумнівні додатки

Пароль

- System -> Security -> Screen Lock, вибрати PIN або пароль (Settings > General > Passcode)
- Мінімум 6 символів
- Переконайтеся, що у вас включена опція «стирати вміст пристрою» після:
  - 10 невдалих спроб введення пароля для iPhone
  - 15 невдалих спроб введення для Android

Шифрування

- Android, починаючи с 4-ої версії, дає можливість зашифрувати сховища апарату. В налаштуваннях знайдіть пункт меню **«Безпека і екран блокування»**, в якому буде підпункт **«Зашифрувати дані»**. Шифрування зазвичай займає від 30 до 60 хвилин, апарат в цей час повинен бути підключений до живлення.
- iPhone шифрує інформацію за замовчуванням.

УВАГА!

Якщо ви зашифрували пристрій і забули пароль, дані, що зберігаються на апараті, стають недоступними.

Автоблокування

- Час бездіяльності, через який смартфон автоматично блокується, в Андроїд можна встановити в настройках: меню «Екран блокування і безпека» - «Налаштування блокування».
- У цій же секції меню є пункт «Блокування кнопкою живлення». Включення цієї опції дозволяє миттєво заблокувати апарат натисканням на кнопку його включення.

Мастхев для смартфона

- Psiphon https://apps.apple.com/us/app/psiphon/id1276263909?ls=1
- www.guardianproject.info/apps/

Одна кнопка!

- Панічна кнопка від http://redpanicbutton.com
  - https://play.google.com/store/apps/details?id=uk.ucsoftware.panicbuttonpro
  - https://apps.apple.com/us/app/red-panic-button/id422029296?ls=1

Якщо його вкрали…

- Android
  - https://play.google.com/store/apps/details?id=com.google.android.apps.adm&hl=ru
- iPhone, iPad, Mac
  - http://www.apple.com/support/icloud/find-my-iphone-ipad-ipod-mac/

Компьютер

Тест

- Які сліди ви залишаєте в мережі? Як зменшити їх число?
- https://myshadow.org/ru/trace-my-shadow

Захист компьютера

- Захист від прямого несанкціонованого доступу
- Шифрування диска
- Шкідливе ПЗ
- Запобігання відстеження нашої активності

Захист компьютера

- Фізичний доступ
  - Пароль входу в систему
  - Блокування в разі відходу від комп'ютера Win + L
  - Контроль доступу та права користувачів основна сесія з обмеженими правами
  - На Windows вимкніть автозапуск пристроїв (Панель керування> Устаткування та звук> Автозапуск> прибрати верхню галочку і внизу натиснути «Зберегти»).

Включене шифрування

- Для Mac – Filevault,
- Для Windows – BitLocker,
- для всіх систем:
  - VeraCrypt

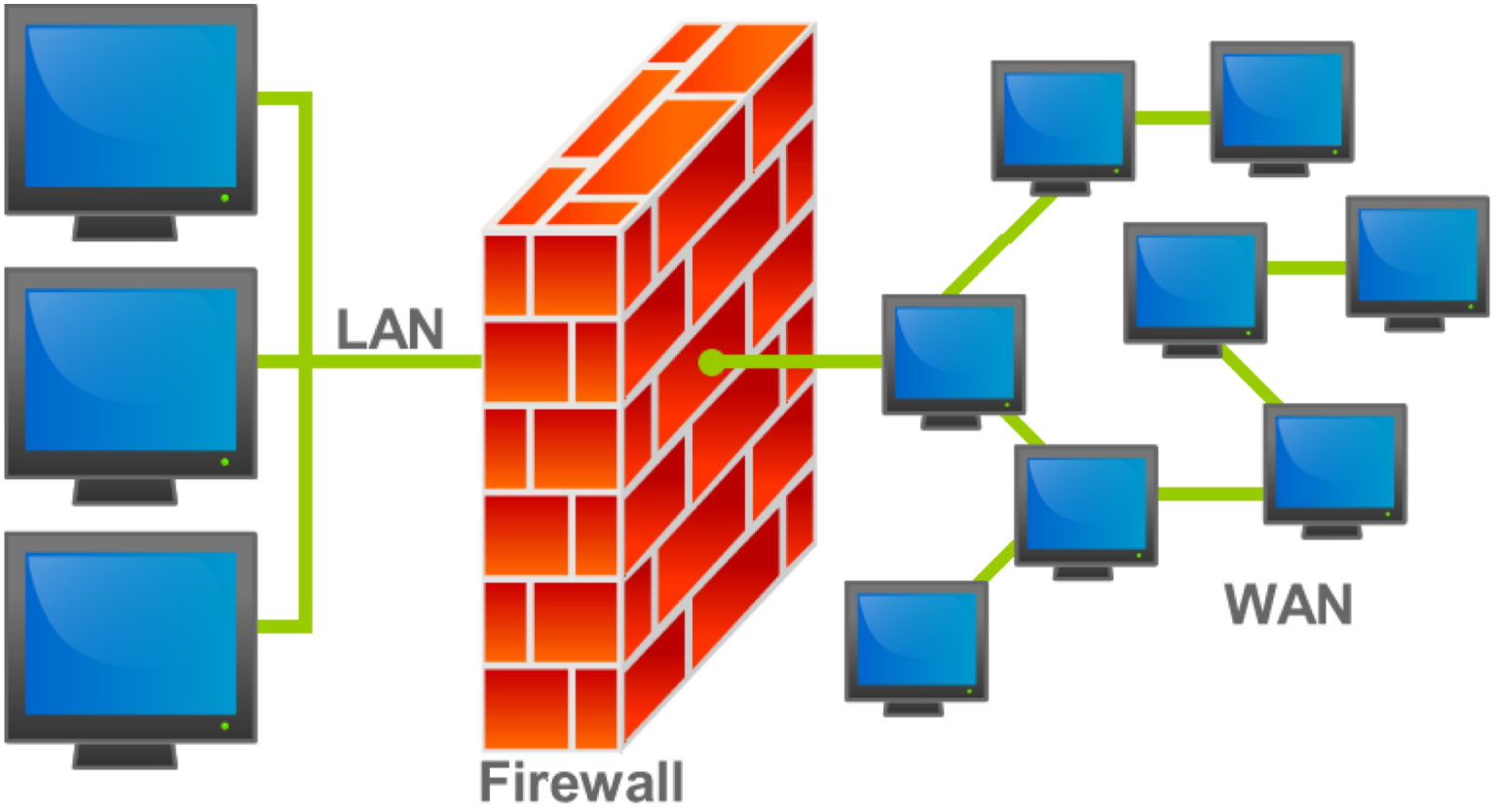
Шкідливе ПЗ

- 90 відсотків зломів відбуваються через те, що людина не дотримувалась звичайної гігієни комунікації, а саме від того, що ви самі на щось натиснули і встановили собі незрозумілу програму.
- Схема проста:
  - Вам приходить лист.
  - Ви його відкриваєте.
  - Ви відкриваєте аттачменті або йдете за посиланням, яке пропонує завантажити і відкрити файл.
  - Шкідливий програмний код вже у вас.

Захист компьютера

- Онлайн вплив
  - Антивірус
    - Безкоштовні – Avast, Bitdefender, AVG, Avira
    - Тести різних антивірусів http://www.av-test.org/en/
  - Щотижневе сканування і регулярне оновлення антивірусів

Firewall (мережевий екран)



Firewall

- Outpost, BitDefender, ZoneAlarm, Norton Internet Security, avast! Internet Security, ESET Smart Security, AVG Internet Security, McAfee Internet Security, ...

- Якщо в пакеті з антивірусом – ОК.

Захист компьютера

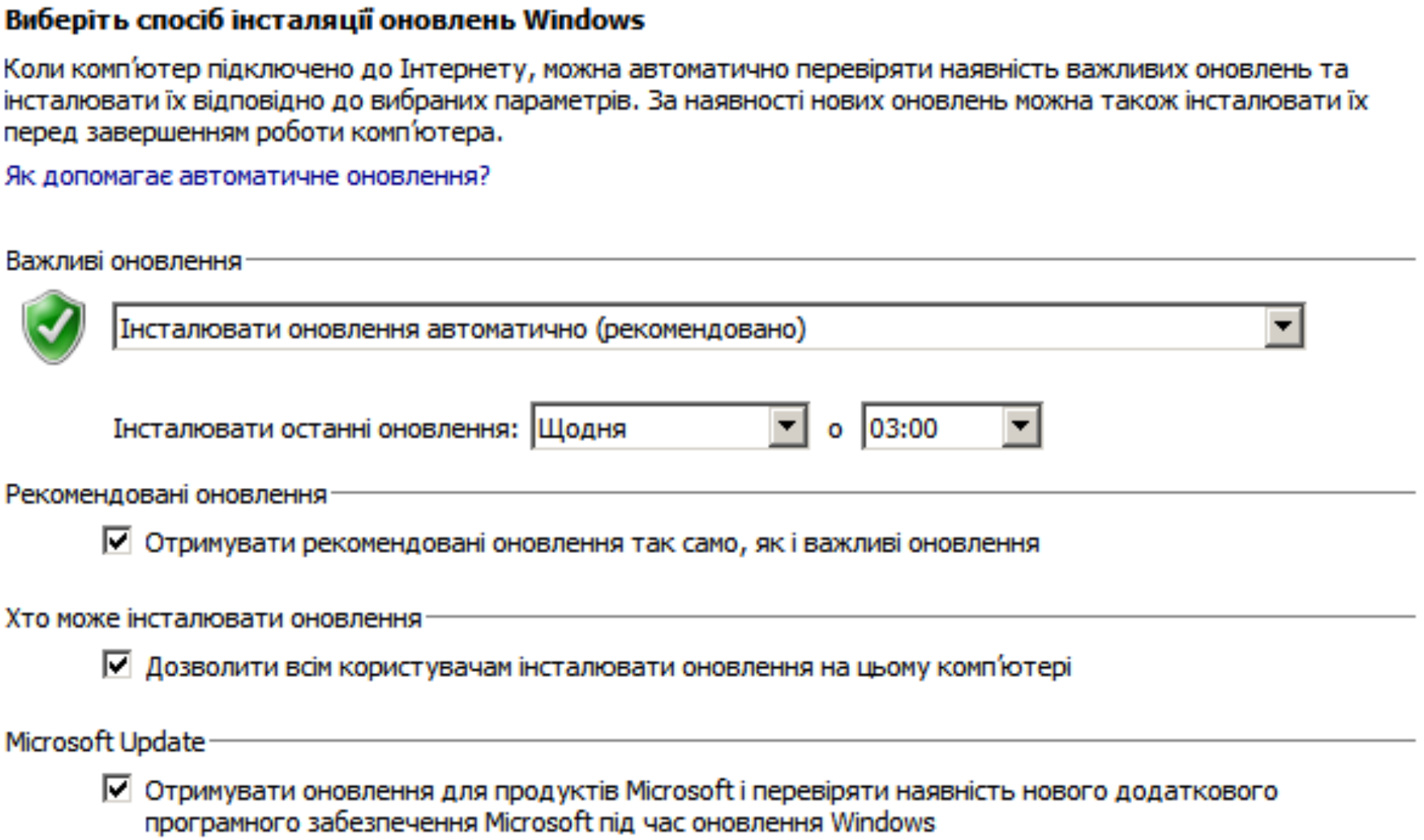
- Інструкція «як легко почистити інфікований шкідливим ПЗ комп'ютер»
  - http://malwaretips.com/blogs/malware-removal-guide-for-windows/
- Сканування на наявність шкідливого ПЗ
  - https://www.malwarebytes.com/antimalware/
  - https://www.microsoft.com/security/scanner/uk-ua/
- Онлайн-антивірус, сканує файл або посилання
  - https://www.virustotal.com/

Spybot

- www.safer-networking.org – викачуємо безкоштовну версію і встановлюємо

- Оновлюємо бази
- Запускаємо сканування ☺

Регулярне оновлення ОС та програм



Додатки для браузера

- У кого IE - встановіть **Chrome** або **Firefox**
- **Adblock** Plus https://adblockplus.org/ru/
- Можливо, **flashblock** https://addons.mozilla.org/ru/firefox/addon/noflash/
- Можливо **NoScript** https://addons.mozilla.org/ru/firefox/addon/noscript/ (увага, заблокує навіть фейсбук)
- **HTTPS Everywhere** https://www.eff.org/https-everywhere
- Шифрування **ZenMate** https://zenmate.com

Облікові записи

Де в нас є облікові записи?

- Пошта
- Мессенджери
- Соціальні мережі
- Адміністративні послуги
- Банківські клієнти
- Інтернет магазини
- Купівля квитків
- Бронювання готелів

Викрадення запису

- Як це працює?
  - Вам приходить лист з попередженням, і проханням ще раз зайти в ваш аккаунт або підтвердити його.
  - Ви йдете за посиланням, вводите логін і пароль.
  - Ваші облікові дані у злоумишеннiков.

Розшифровка коротких лінків

- https://longurl.info - тут можемо подивитися куди веде справжнє посилання, заховане за скороченим посиланням типу bit.ly, goo.gl тощо.
- https://urlex.org – ще один сервіс
- https://chrome.google.com/webstore/detail/longurl/cmkcdiijleanafkljglfjihodbkhloej - плагін для Chrome

Паролі

qwerty

Дуже погані паролі

- Імена
- Прості слова
- Номер телефону
- Дата народження
- І т.і.

Паролі

- Паролі не менше 12 символів, що складаються з малих і великих літер, спецсимволов, і цифр.

Rjycnsnewbz Erhf]ys1996

КонституціяУкраїни1996

в англійській розкладці

Паролі

- Не повторюйте паролі для різних облікових записів
- Окремий пароль для блокування комп'ютера
- Менеджер паролів https://lastpass.com/ru/

Перевіряємо стійкість пароля

https://howsecureismypassword.net/

Чи був мій мейл серед витоків даних облікових записів?

- https://haveibeenpwned.com

Двофакторна авторизація

- Двофакторна авторизація при вході в профіль https://brainstation.io/cybersecurity/two-factor-auth
- Онлайн-банкінг
- Google
- Facebook
- Багато інших сервісів

Захист облікових записів

GOOGLE AUTHENTICATOR

- Google authentificator

Комунікація

Електронна і голосова

Мессенджери

- Надійні
  - Signal
  - WhatsApp
- Частково надійні
  - Telegram
  - FaceTime
  - iMessage
- Ненадійні
  - Skype
  - Viber

Захист голосової и мережевої коммунікації

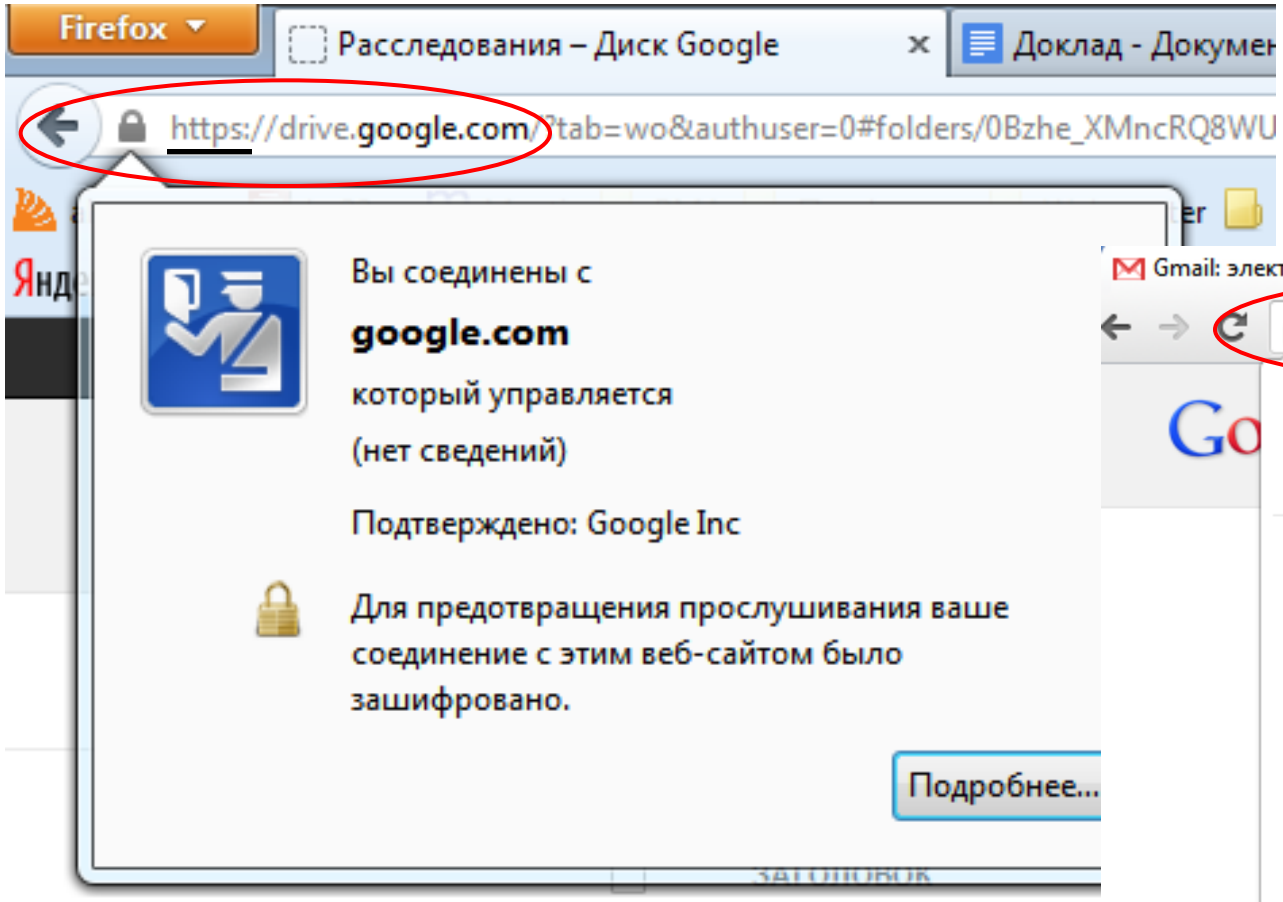
- НІЯКИХ розмов по телефону!
- НІЯКИХ розмов по скайпу і вайберу
- Signal
- Шифрування пошти та надісланих файлів
- Шифрування і анонімізація трафіку браузера

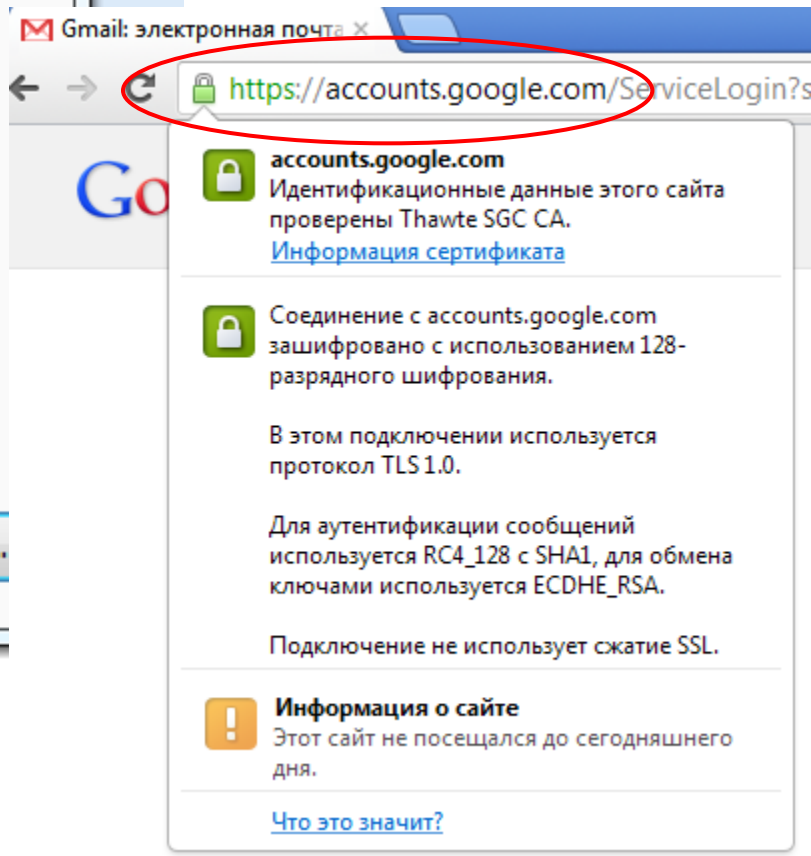
Шифрування пошти та надісланих файлів

- Pretty Good Privacy (PGP)
  - PC
    - https://www.mailvelope.com/
  - MAC
    - https://gpgtools.org/
- End to end encryption
  - https://www.mesince.com/en-us

SSL- з'єднання

SSL

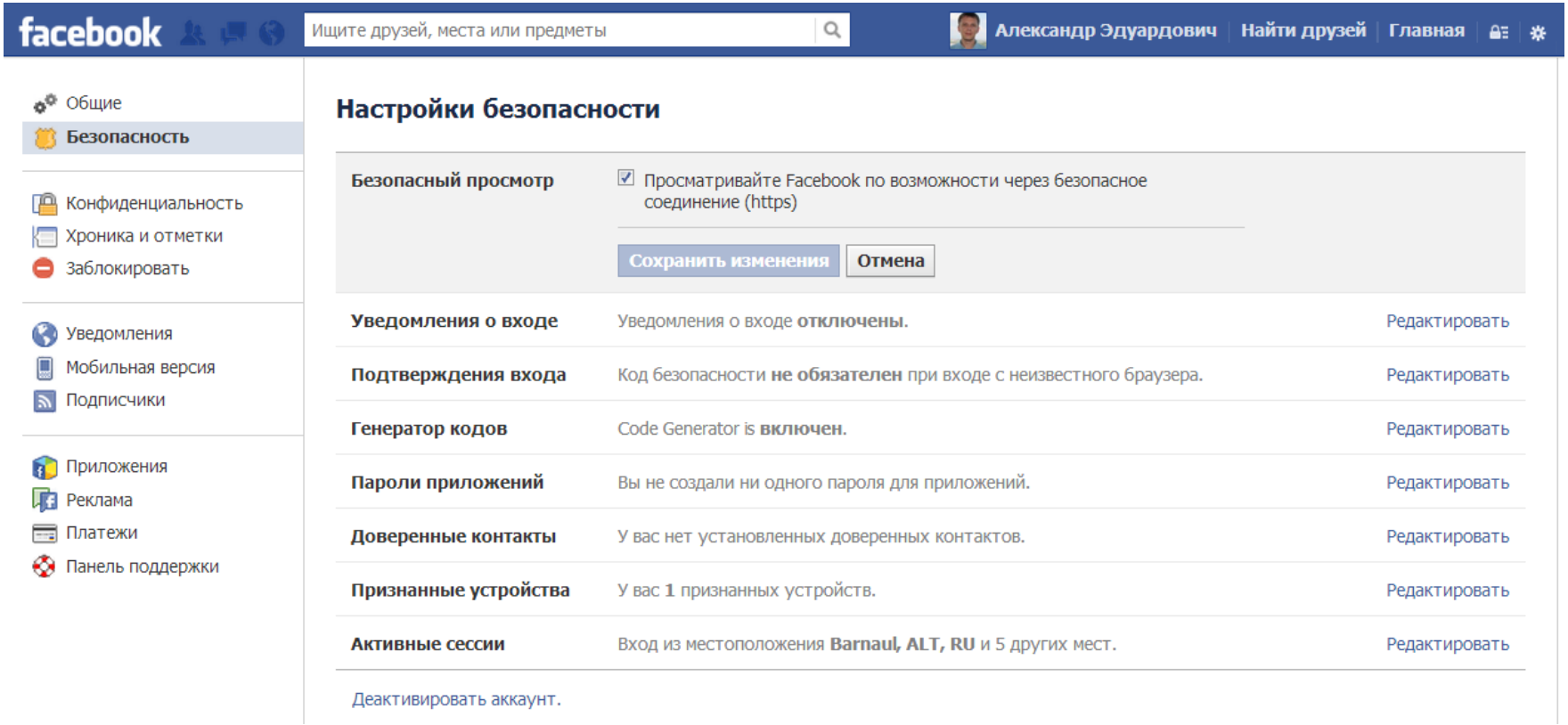




Захист та шифрування сайту

- Отримання цифрового сертифіката шифрування підключення до сайту https://letsencrypt.org забезпечить надійність передачі даних і обмежить зловмисникам можливість сісти на трафік.
- https://store.wotrus.com SSL-сертифікати (для HTTPS)

facebook



Шифрування і анонімізація трафіку браузера

- TOR браузер – https://www.torproject.org/
- Безкоштовний VPN – https://zenmate.com.ru/
- Безкоштовний VPN – https://psiphon.ca/ru/

Сайти двійники

- Цілі створення
  - Комунікація і поширення ідей від імені чужої організації
  - Поширення фейків
  - Провокація і компрометація журналіста

Сайти двійники - метрики

- Вік домена
- ТІЦ
- Відвідуваність
- Кількість посилань
- Сервіс http://pr-cy.ru

Сайти двійники – хостинг

- Реєстраційні дані
- https://www.whois.net/
- https://www.whoisxmlapi.com/
- http://www.whoishostingthis.com/
- https://whoisology.com/

Робота с даними

Очищаємо вільний простір диска

- Ccleaner: завантажуємо і встановлюємо www.piriform.com/ccleaner
- Інструменти - очищення диска, тут вибираємо потрібні опції (УВАЖНО!) І запускаємо очистку

Відновлення видалених файлів

- Recuva: завантажуємо і встановлюємо www.piriform.com/recuva
- Запускаємо сканування і дивимося свої «видалені» файли ☺
- Відновлюємо якийсь із «видалених» файлів

Зберігання та надійне видалення даних

- Всю важливу інформацію в зашифрованому вигляді зберігати на зовнішніх інформаційних накопичувачах без доступу до мережі
- http://eraser.heidi.ie/ - програма для повного і безповоротного видалення даних з комп'ютера.

Інструменти зберігання та обміну

- Google Drive
- Google Docs
- Dropbox
- iCloud
- https://dropmefiles.com/
- https://www.fex.net

Посібники та домашнє читання

- Інструкції на всі випадки життя https://ssd.eff.org/ru/index
- Комплекс інструкцій з цифрової безпеки https://securityinabox.org/ru/
- Конфіденційність в мережі інтернет для журналістів https://irrp.org.ua/wp-content/uploads/2017/11/Konfydentsyalnost-v-sety-Ynternet-dlya-zhurnalystov.pdf
- Інформаційна самооборона https://team29.org/keep_privacy/

Дякую за увагу!

Олег Хоменок,
oleg.khomenok@gmail.com

https://www.facebook.com/oleg.khomenok