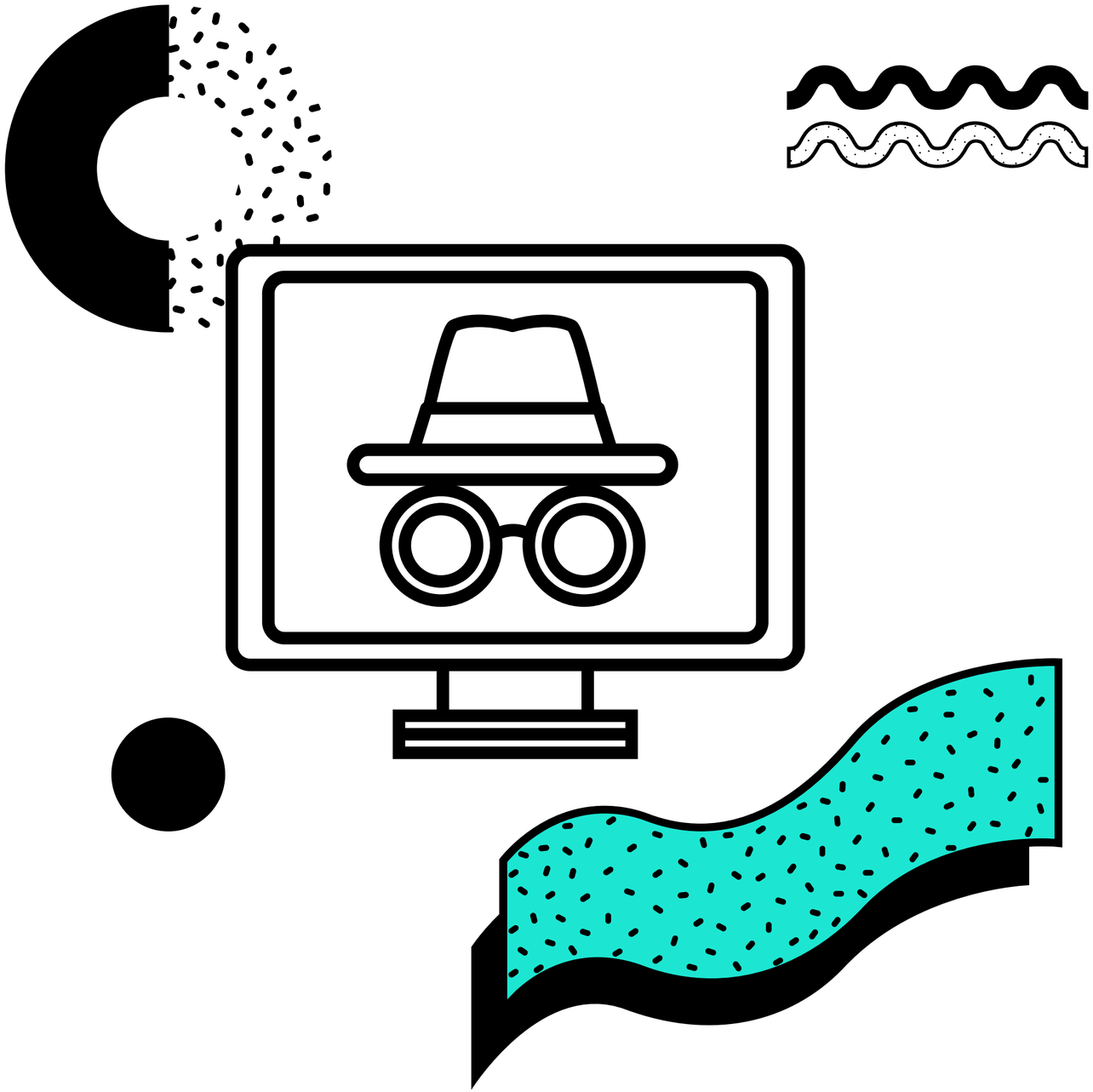


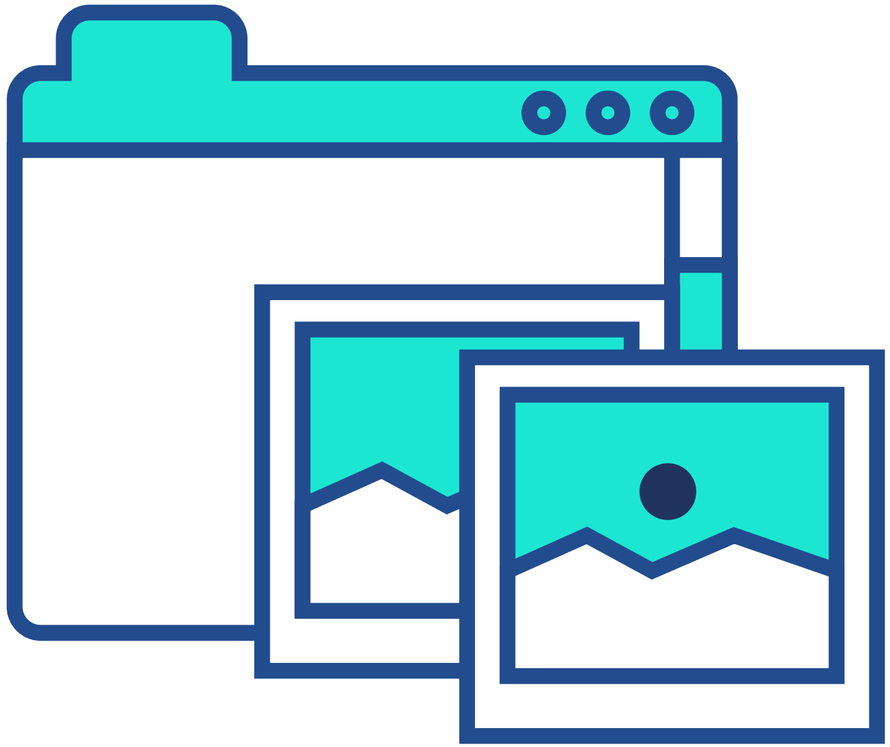
КРИПТОГРАФІЯ

ПРОЕКТ

Презентація студентки групи ПМ-81,
Пороскун Олени

2021

ПРОТОКОЛИ ТАЄМНОГО ГОЛОСУВАННЯ



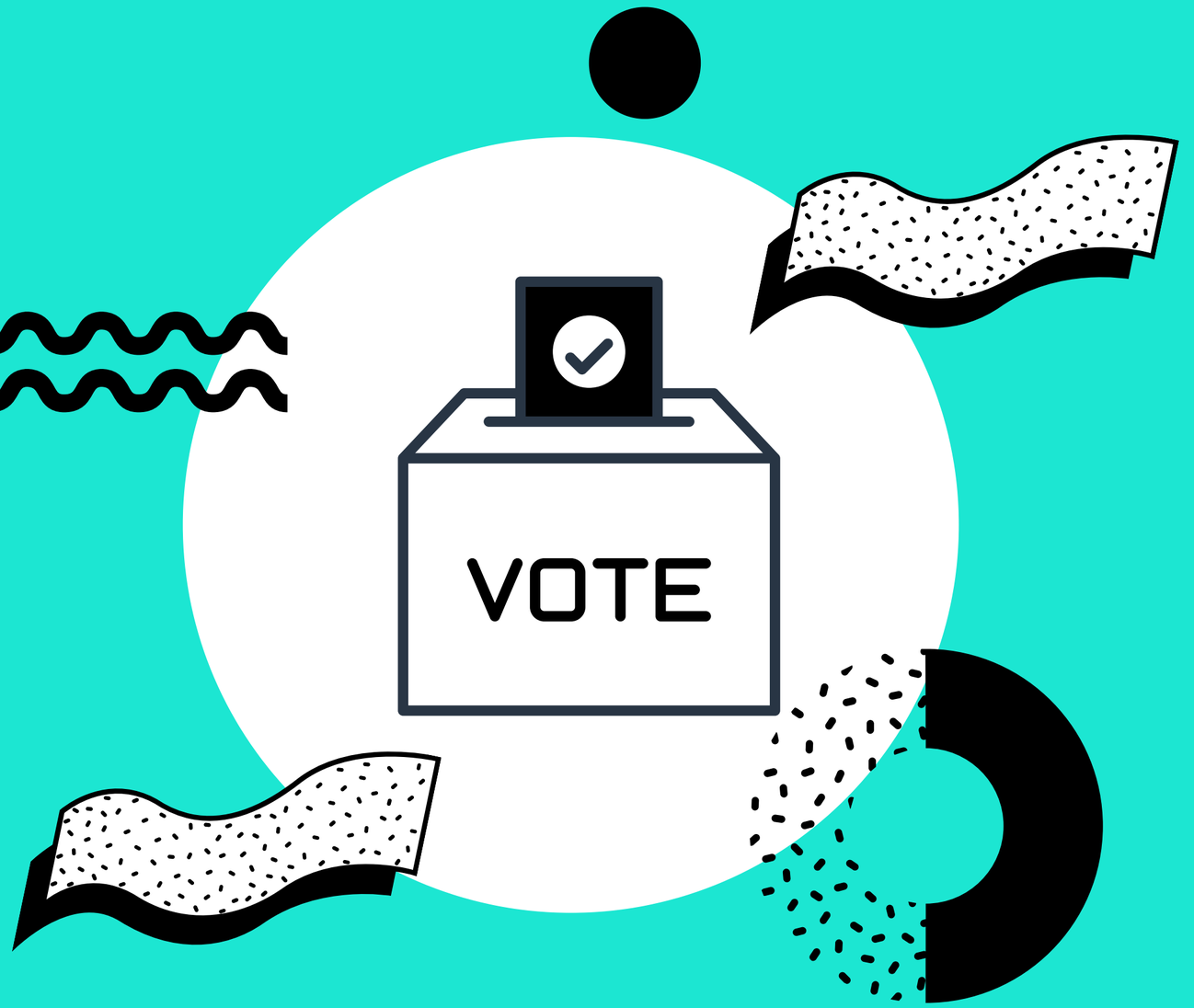
Пункт 1
Електронне голосування

Пункт 2
Протоколи таємного голосування

Пункт 3
Висновок

ЕЛЕКТРОННЕ ГОЛОСУВАННЯ

electronic voting, e-voting

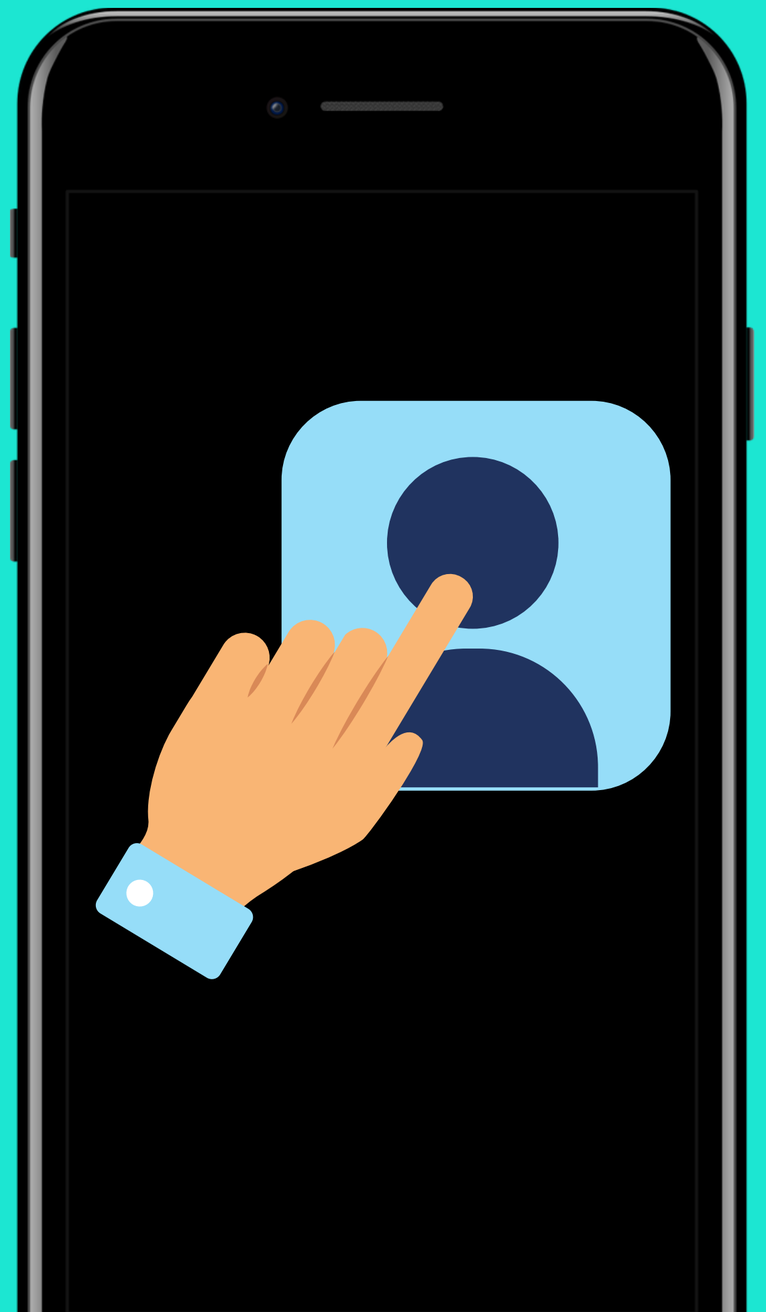


Пункт 1

Термін "електронне голосування" позначає використання електронних засобів голосування на виборах / референдумах.

Системи електронного голосування активно застосовуються в Бельгії, Бразилії, Індії, Венесуелі, США та Естонії.

Протоколи таємного голосування



Пункт 2

Протоколи таємного голосування — протоколи обміну даними для реалізації безпечного таємного електронного голосування через Інтернет за допомогою комп'ютерів, телефонів або інших спеціальних обчислювальних машин. Це напрямок криптографії все ще розвивається, але вже застосовується на практиці.

Асиметричні алгоритми шифрування

Ефективні системи криптографічного захисту даних, які також називають криптосистемами з відкритим ключем.

В таких системах для зашифровування даних використовують один ключ, а для розшифровування — інший (звідси і назва — асиметричні).

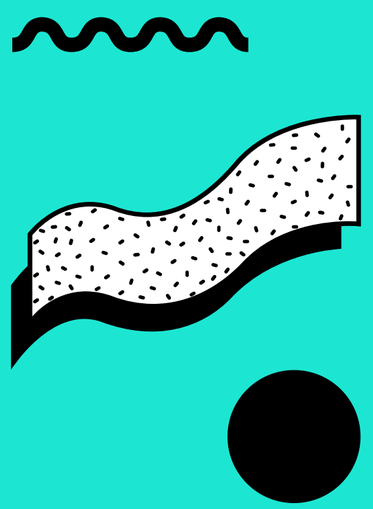
Принцип роботи асиметричної криптосистеми

Електронний цифровий підпис

Вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача.

Електронний цифровий підпис(ЕЦП) накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.

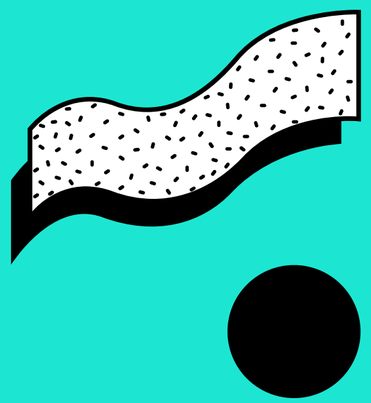
Вимоги до систем таємного голосування



Обов'язкові:

- ніхто, крім голосуючого, не повинен знати його вибір;
- тільки легітимні учасники можуть проголосувати, і притому тільки один раз;
- рішення голосуючого не може бути таємно або явно ким-небудь змінено (крім, можливо, ним самим).

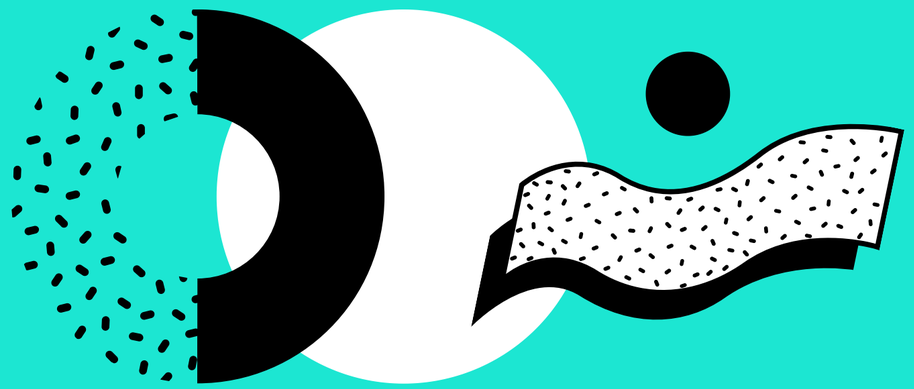
Вимоги до систем таємного голосування



Бажані:

- кожен легітимний учасник може переконатися, що його голос зарахований;
- кожен легітимний учасник може передумати і змінити свій вибір протягом певного періоду часу;
- система повинна бути захищена від продажу голосів виборцями;
- неможливо відстежити, звідки дистанційно проголосував виборець;
- можна дізнатися, хто брав участь в голосуванні, а хто — ні і тд.

ПРОСТИЙ ПРОТОКОЛ ТАЄМНОГО ЦИФРОВОГО ГОЛОСУВАННЯ



Простий алгоритм електронного голосування по суті являє собою листування з електронними підписами між виборчим комітетом та безліччю виборців.

ПОЗНАЧЕННЯ

Нехай тут і далі:

A — агентство, що проводить електронне голосування (*англ*. *Agency*),

E — виборець, легітимний учасник голосування (*англ*. *Elector*),

B — цифровий бюлетень.

B може містити число, ім'я кандидата, розгорнутий текст або які-небудь інші дані, що повідомляють про вибір E, які верифікують його або необхідні для посилення безпеки протоколу.

Алгоритм

Крок 1. **A** викладає списки можливих виборців.

Крок 2. Користувачі, в числі яких і **E**, повідомляють про бажання брати участь у голосуванні.

Крок 3. **A** викладає легітимні списки виборців.

Кроки 1-3 обов'язкові. Основна мета — визначення та оголошення числа активних учасників n. Хоча деякі з них можуть не брати участь, а деякі і зовсім не існувати («мертві душі», зловмисно внесені **A**), можливість маніпулювання голосуванням у **A** помітно знижена. Надалі ці кроки будуть вважатися за один крок «затвердити списки».

Крок 4. **A** створює відкритий і закритий ключ a_{public} $a_{private}$ викладає в загальний доступ a_{public}. Хто завгодно може зашифрувати повідомлення за допомогою a_{public} , але розшифрувати його зможе тільки **A**.

Алгоритм

Крок 5. E

- створює власні публічний і приватний ключі ЕЦП e_{public} $e_{private}$, потім публікує відкритий ключ. Хто завгодно може перевірити документ **E**, але підписати його - тільки сам виборець. Цей крок пропускається, якщо **A** вже знає електронні підписи виборців (наприклад, вони були згенеровані при реєстрації в системі).
- формує повідомлення **B**, де тим або іншим способом висловлює свою волю
- підписує повідомлення особистим закритим ключем $e_{private}$
- шифрує повідомлення відкритим ключем a_{public}
- відправляє шифроване повідомлення **A**

Крок 6. A

- збирає повідомлення
- розшифровує їх за допомогою лежачого у відкритому доступі e_{public}
- підраховує їх і публікує результати

Особливості, переваги та недоліки

Цей протокол надзвичайно простий, тим не менш, його достатньо, щоб захиститися від зовнішнього втручання, підробки голосів і дискредитації легітимних виборців.

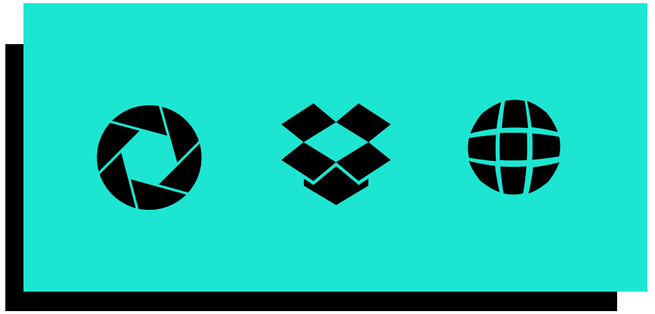
ІНШІ ПРОТОКОЛИ

Протокол двох агентств

Протокол Sensus

Протокол Фудзиока-Окамото-Охта

Протокол He-Su



На даний момент протокол Фудзіока-Окамото-Охта (а також його модифікації, включаючи і Sensus) є одним з найбільш перевірених протоколів дистанційного електронного голосування. Саме його варіація була застосована на електронних виборах в Естонії.

Існує безліч інших протоколів та криптографічних примітивів з різними специфічними властивостями. Вони не так широко відомі і застосовуються, щоб впоратися з якими-небудь особливими обмеженнями середовища або досягти додаткових цілей.

ВИСНОВОК

Прогрес техніки дозволив задуматися про голосування через Інтернет тільки близько 20 років тому, тому даний розділ криптографії все ще розвивається. По ньому немає загальновизнаних книг, і жоден протокол ще не отримав переважну підтримку фахівців.

ДЖЕРЕЛА

- https://habr.com/ru/post/436560/
- http://itconf.kpfu.ru/Lists/List1/Attachments/1397/Кудрякова835.pdf
- https://uk.wikipedia.org/wiki/Протоколи_таємного_голосування
- https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema15/tema15_3
- https://amp.ww.google-info.org/4818616/1/protokoly-taynogo-golosovaniya.html
- https://www.youtube.com/watch?v=srbW1L0oRm8
- А. М. Кандарова, Науч. руковод. – канд. техн. наук, доцент Т. А. ИВАНОВА, Уфимский государственный авиационный технический университет // Системы тайного он-лайн голосования URL:https://www.ugatu.su/media/winterSchoolSeminar/article/2020-09-04/2020-shablon-rints_1.docx
- https://uk.wikipedia.org/wiki/Електронний_цифровий_підпис
- https://uk.wikipedia.org/wiki/Асиметричні_алгоритми_шифрування
- https://aceproject.org/ace-ru/focus/e-voting/what-is-e-voting
- https://www.kommersant.ru/doc/3236500