Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»
(Университет ИТМО)

ИТМО

Выпускная квалификационная работа

Разработка интерактивной методики оценки эффективности систем цифровой подписи на основе библиотеки PyCryptodome

Факультет безопасности информационных технологий
Образовательная программа Технологии защиты информации
Направление подготовки (специальность) 10.03.01 Информационная безопасность
Выполнил студент: Гутник Дмитрий Вячеславович, N34491
Научный руководитель: доцент ФБИТ, к.т.н., Таранов Сергей Владимирович
Санкт-Петербург, 2023

Актуальность

- Увеличение генерации цифровых подписей (28 миллионов)*
- Увеличение количества выданных сертификатов (13,8 миллионов)*
- Увеличение количества выданных меток времени (117 миллионов)*

* Источник: GlobalSign, 2021

Цель и задачи

Цель: повышение эффективности применения алгоритмов цифровой подписи путём рекомендации подходящего алгоритма в зависимости от условий применения.

Задачи:

1. Анализ и разделение на виды актуальных алгоритмов цифровой подписи
2. Разработка интерактивной методики оценки эффективности систем цифровой подписи на основе библиотеки PyCryptodome
3. Разработка рекомендаций к практическому применению методики

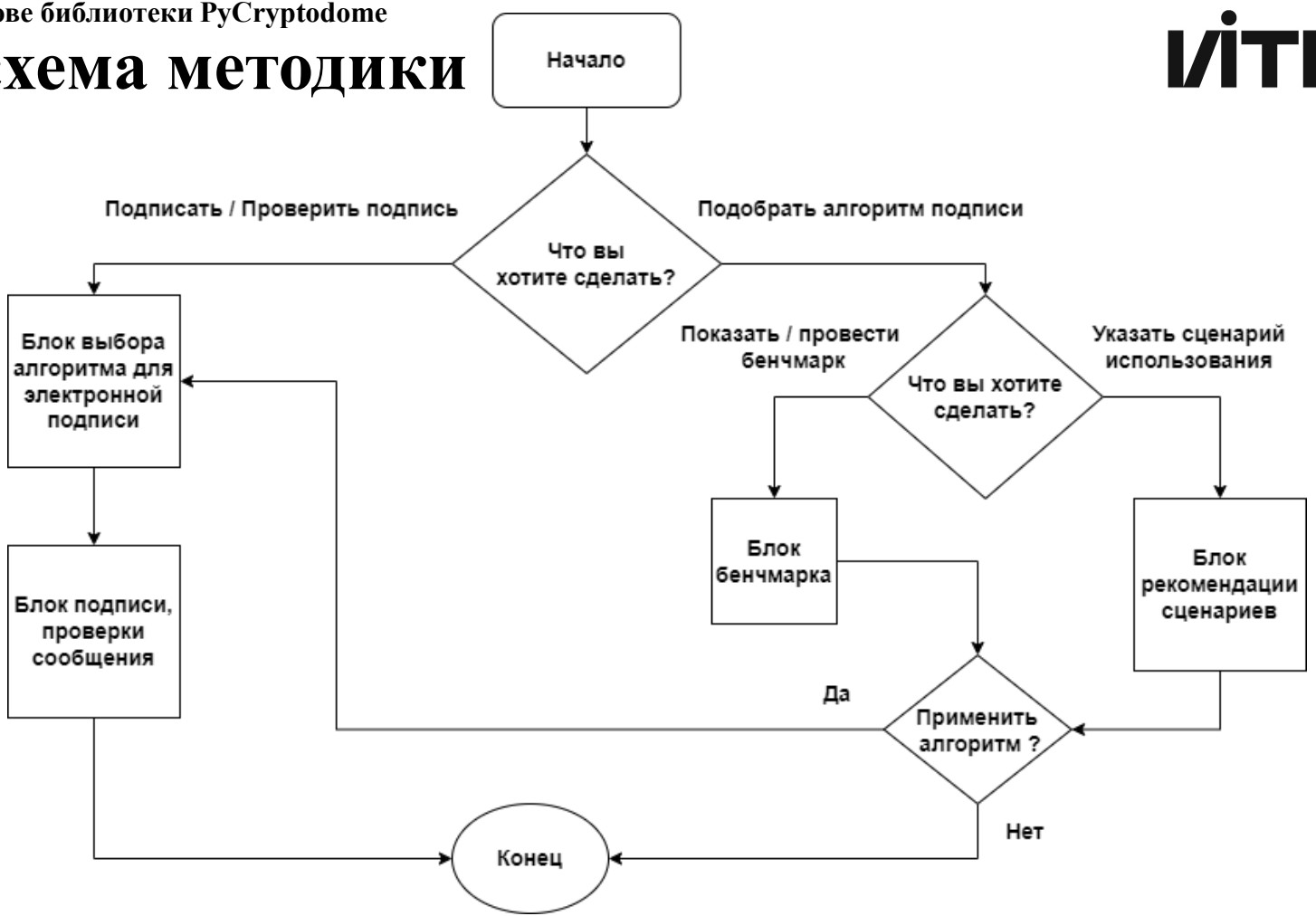
Критерии рекомендации сценариев

- скорость работы алгоритма
- размер подписи
- размер ключа
- распространённость алгоритма в существующем ПО

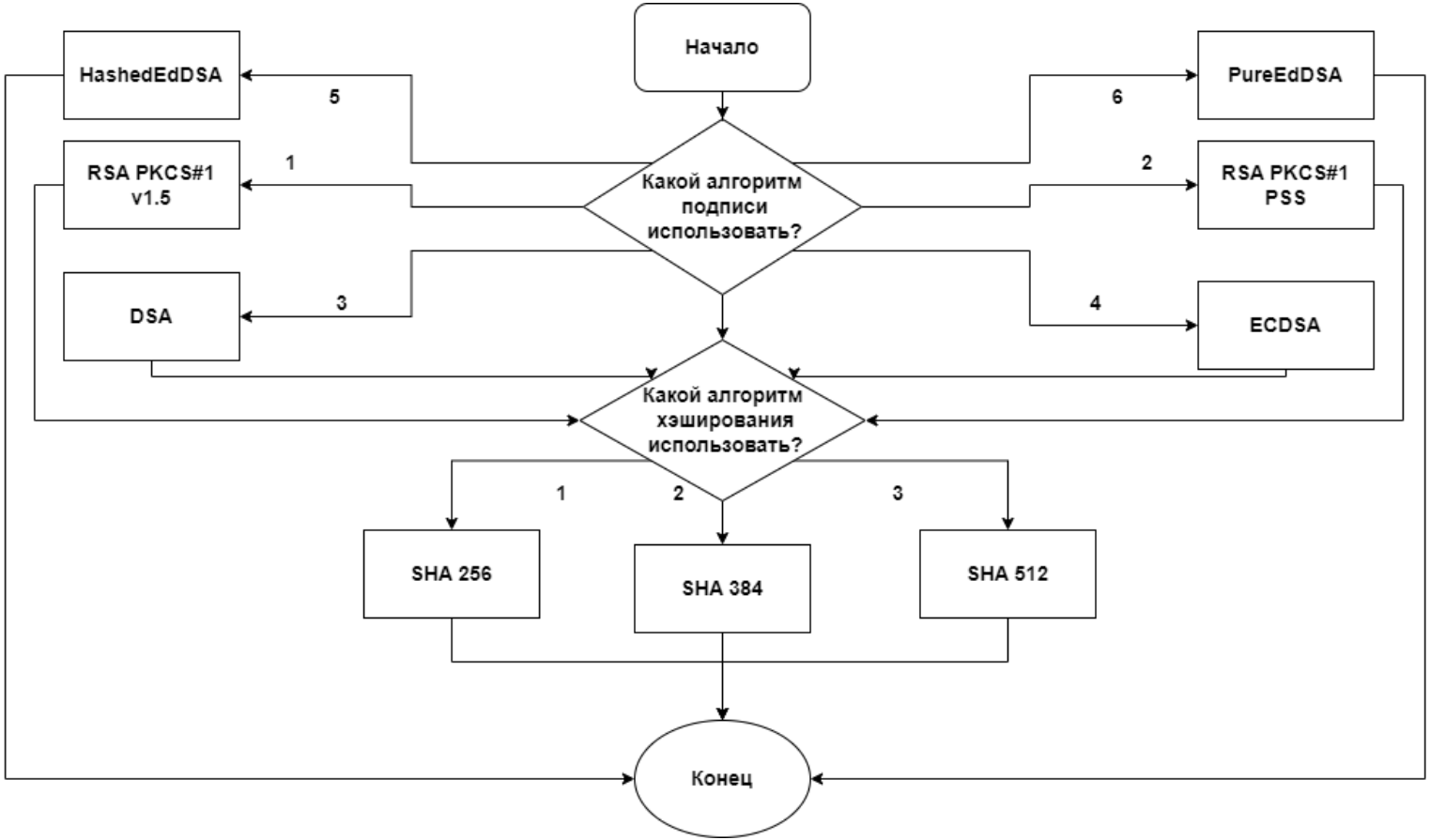
Рассмотренные атаки

- коллизионные атаки
- атаки грубой силы
- атаки на алгоритм дополнения
- адаптивная атака с выбранным зашифрованным текстом
- атака с малыми значениями секретной экспоненты
- атаки по сторонним каналам
- атаки связанные с псевдослучайными числами
- и другие

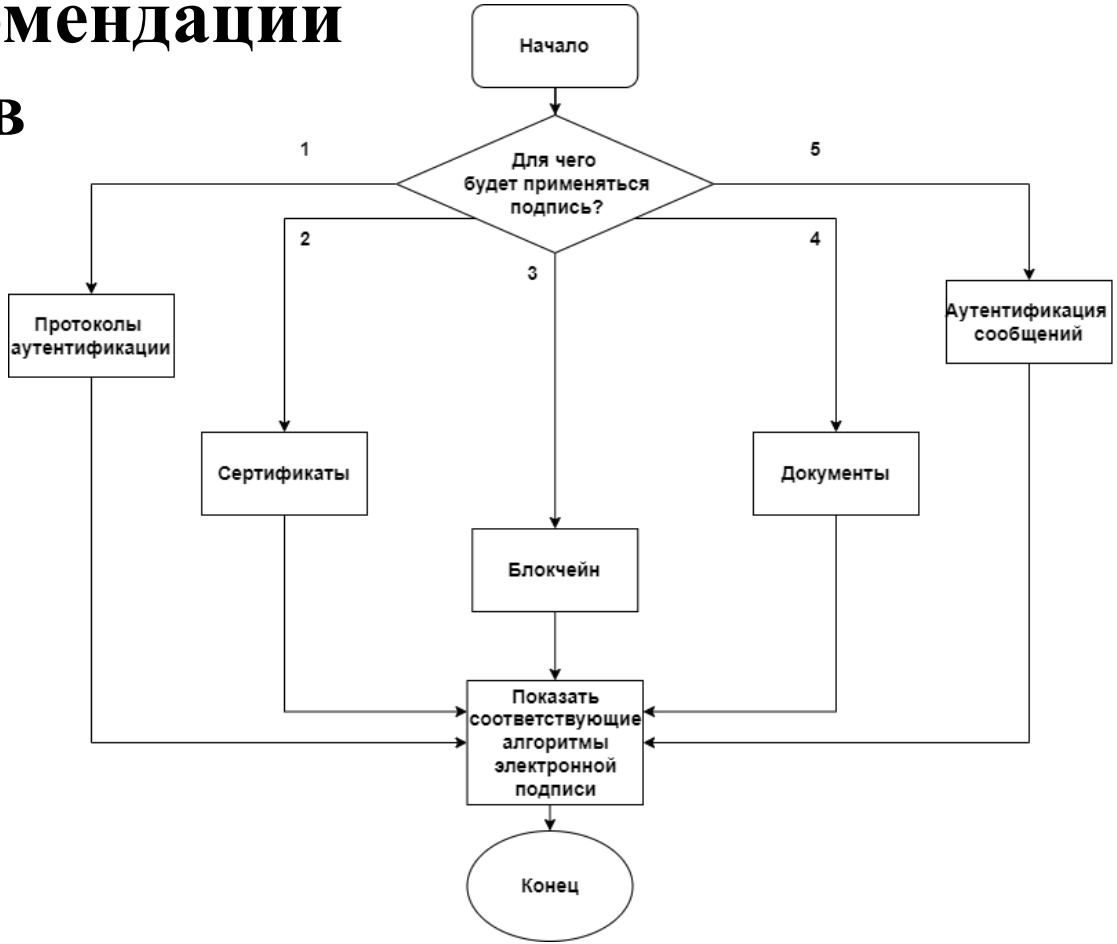
Блок схема методики



Блок выбора алгоритмов



Блок рекомендации сценариев



Тест скорости работы алгоритмов с импортом ключа

Импорт ключа				
алгоритм	Хэш	подпись, сек	проверка, сек	всего, сек
rsa_v1_5	SHA256	0.03400	0.00351	0.03752
rsa_v1_5	SHA384	0.03355	0.00300	0.03655
rsa_v1_5	SHA512	0.03350	0.00200	0.03551
rsa_pss	SHA256	0.03275	0.00300	0.03575
rsa_pss	SHA384	0.03227	0.00400	0.03627
rsa_pss	SHA512	0.03233	0.00255	0.03488
dsa	SHA256	0.08068	0.08228	0.16296
dsa	SHA384	0.08088	0.08126	0.16214
dsa	SHA512	0.07934	0.08100	0.16034
ecdsa	SHA256	0.00200	0.00651	0.00852
ecdsa	SHA384	0.00200	0.00554	0.00755
ecdsa	SHA512	0.00201	0.01552	0.01753
eddsa	SHA512	0.00101	0.00200	0.00301
pure_eddsa	-	0.00001	0.00200	0.00200

Тест скорости работы алгоритмов с созданием ключа

Создание ключа				
алгоритм	Хэш	подпись, сек	проверка, сек	всего, сек
rsa_v1_5	SHA256	1.25953	0.00652	1.26605
rsa_v1_5	SHA384	0.24042	0.00600	0.24643
rsa_v1_5	SHA512	0.85727	0.00651	0.86378
rsa_pss	SHA256	0.64162	0.00600	0.64762
rsa_pss	SHA384	1.04822	0.00552	1.05374
rsa_pss	SHA512	0.77940	0.00601	0.78541
dsa	SHA256	11.39181	0.08569	11.47750
dsa	SHA384	7.66034	0.08461	7.74495
dsa	SHA512	0.20279	0.08482	0.28761
ecdsa	SHA256	0.00251	0.00898	0.01149
ecdsa	SHA384	0.00201	0.00851	0.01052
ecdsa	SHA512	0.00251	0.00851	0.01102
eddsa	SHA512	0.00100	0.00601	0.00701
pure_eddsa	-	0.00150	0.00601	0.00752

Примеры размерности подписей и ключей

Алгоритм	Размер подписей, байт	Размер закрытых ключей, байт	Размер открытых ключей, байт
DSA	56	882	1189
ECDSA	132	390	272
EdDSA	64	120	114
Pure EdDSA	64	120	114
PKCS#1 v1.5	256	1678	450
PKCS#1 PSS	256	1674	450

Аналоги

	Разработанная методика	Cryptoy	Методика Жданова	Cryptool
Несколько алгоритмов подписи	+	-	-	-
Ассиметричные алгоритмы шифрования	+	-	-	+
Оптимально подобранные настройки алгоритмов	+	-	-	+
Подпись, проверка подписи	+	-	-	+
Возможность использования кода алгоритма вне программы	+	-	+	-

Выводы

Выполнены задачи:

1. Проанализированы и разделены на виды актуальные алгоритмы цифровой подписи
2. Разработана интерактивная методика оценки эффективности систем цифровой подписи на основе библиотеки PyCryptodome
3. Разработаны рекомендации к практическому применению методики

Цель достигнута, задачи выполнены.

Спасибо
за внимание!

ITMO more than a UNIVERSITY