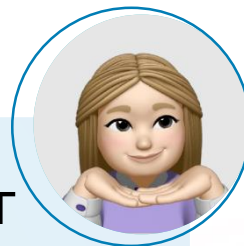


Прикладная криптография. С чего начать и что учитывать.



Кто ты такая и зачем тебя слушать



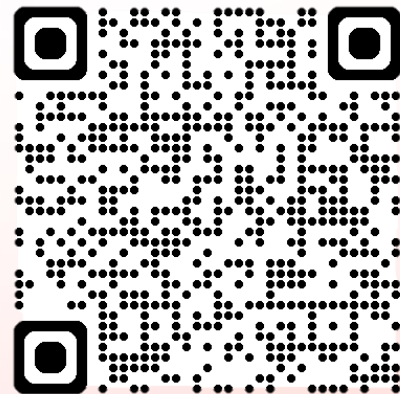
Анкель Лихтенберг

Системный аналитик

АО «ИнфоТеКС», АНО ИТЦ ЦК

Криптография и квантовые технологии

Шпаргалка по криптографии: что
делать, если попал в проект с
криптографами



Почему криптография нужна в разработке

Конфиденциальность

свойство безопасности информации, при котором доступ к ней осуществляют только субъекты доступа, имеющие на него право



Целостность

термин, означающий, что данные не были изменены при выполнении какой-либо операции над ними, будь то передача, хранение или отображение

Аутентичность

подлинность, полнота и точность информации, означающая, что информация: была создана законными участниками информационного процесса; не подвергались случайным или преднамеренным искажениям



Неотказуемость

состояние информации, при котором субъект не может отказаться от того действия, которое имело место быть



Сценарии для разработки

- ◁ Защищённое хранение
 - ◁ как хранить данные
 - ◁ и почему только шифрования не достаточно
- ◁ Установление безопасного соединения
 - ◁ кому и почему можно доверять
 - ◁ что и как защищаем
- ◁ Подпись электронных документов
 - ◁ как и чем подписать, чтобы все поверили



Я понял, что мне не сбежать

Какая бывает криптография

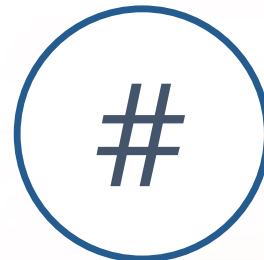
01. Симметричная



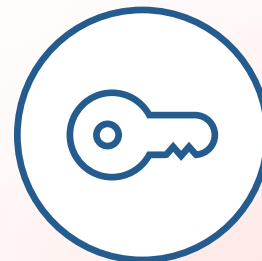
02. Асимметричная



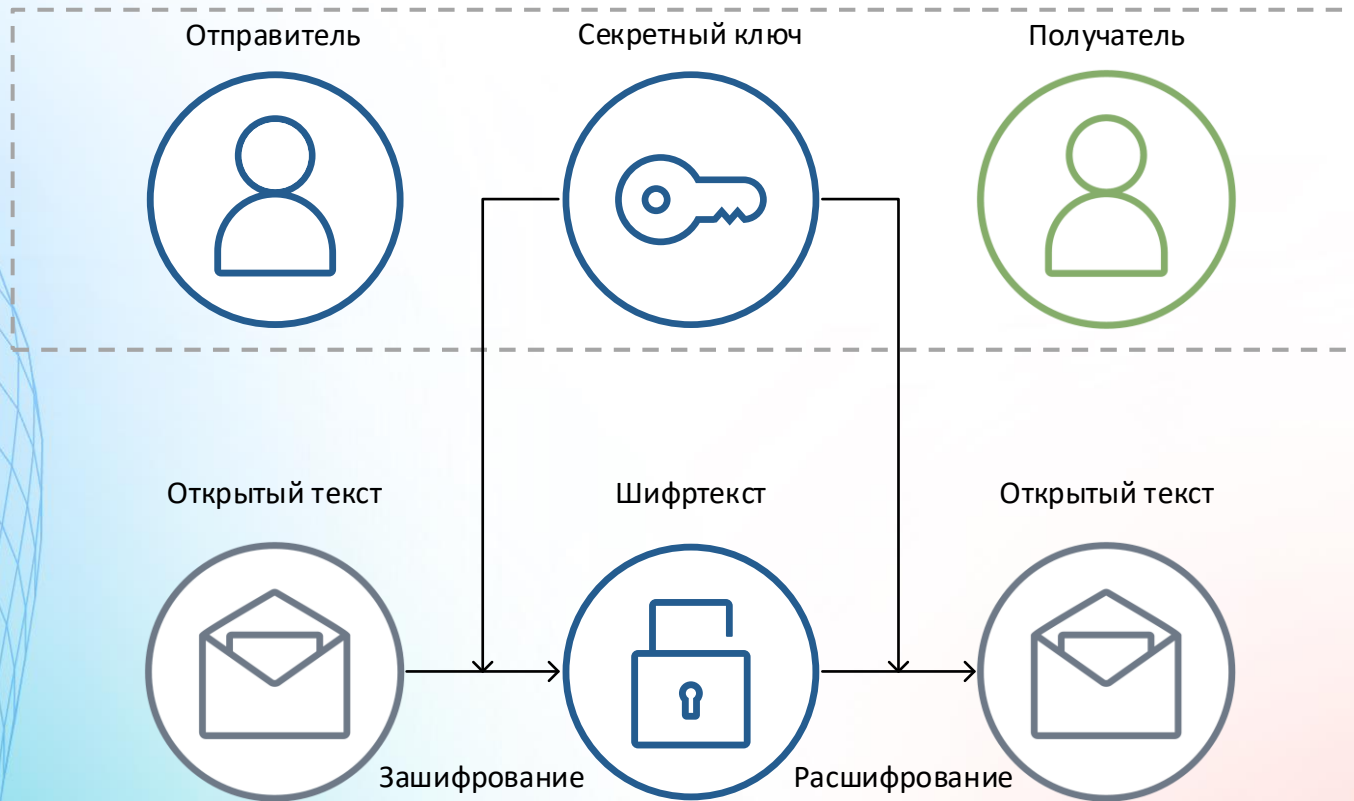
03. Бесключевая - хэши



04. Выработка общего секрета



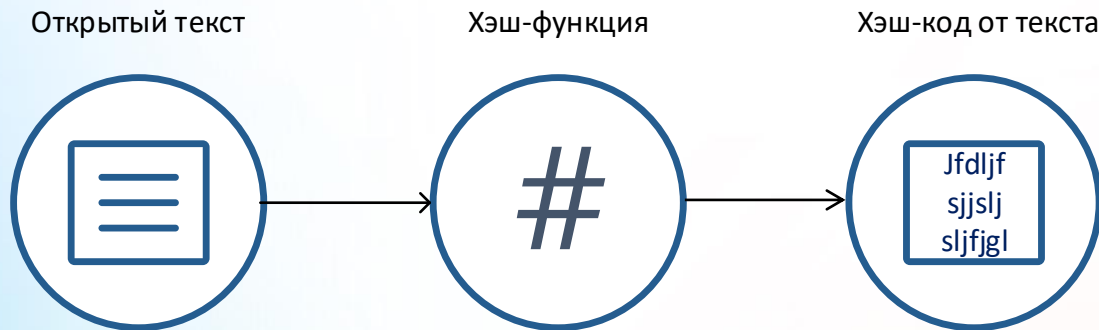
Симметричная криптография



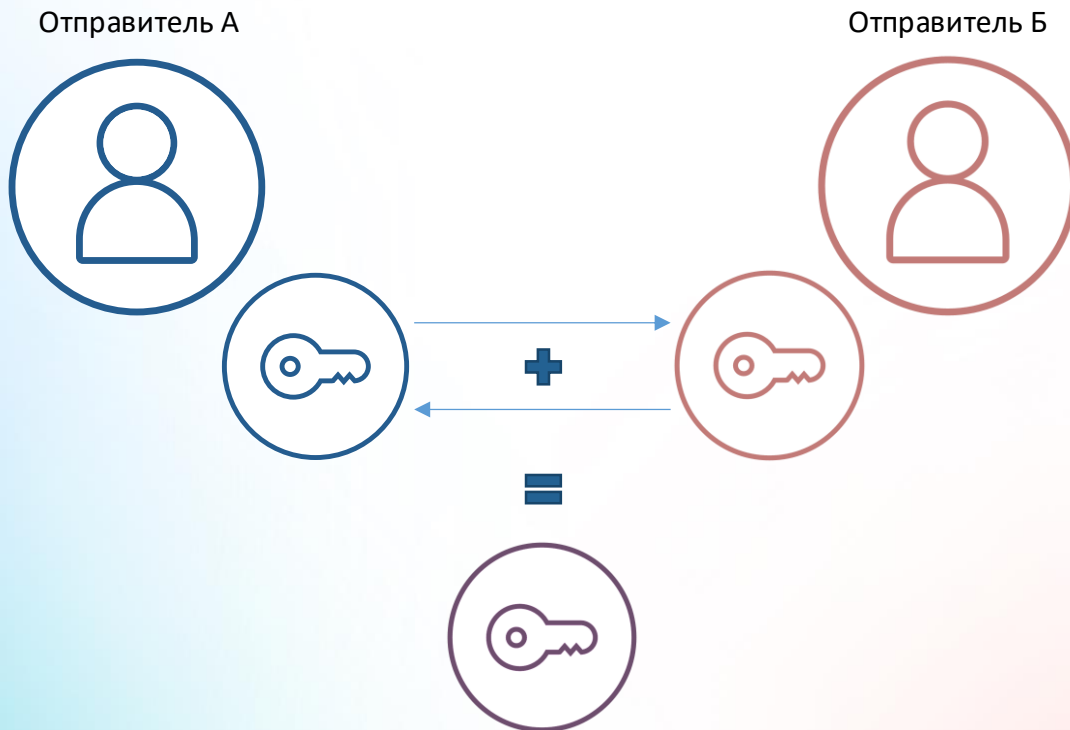
Асимметричная криптография



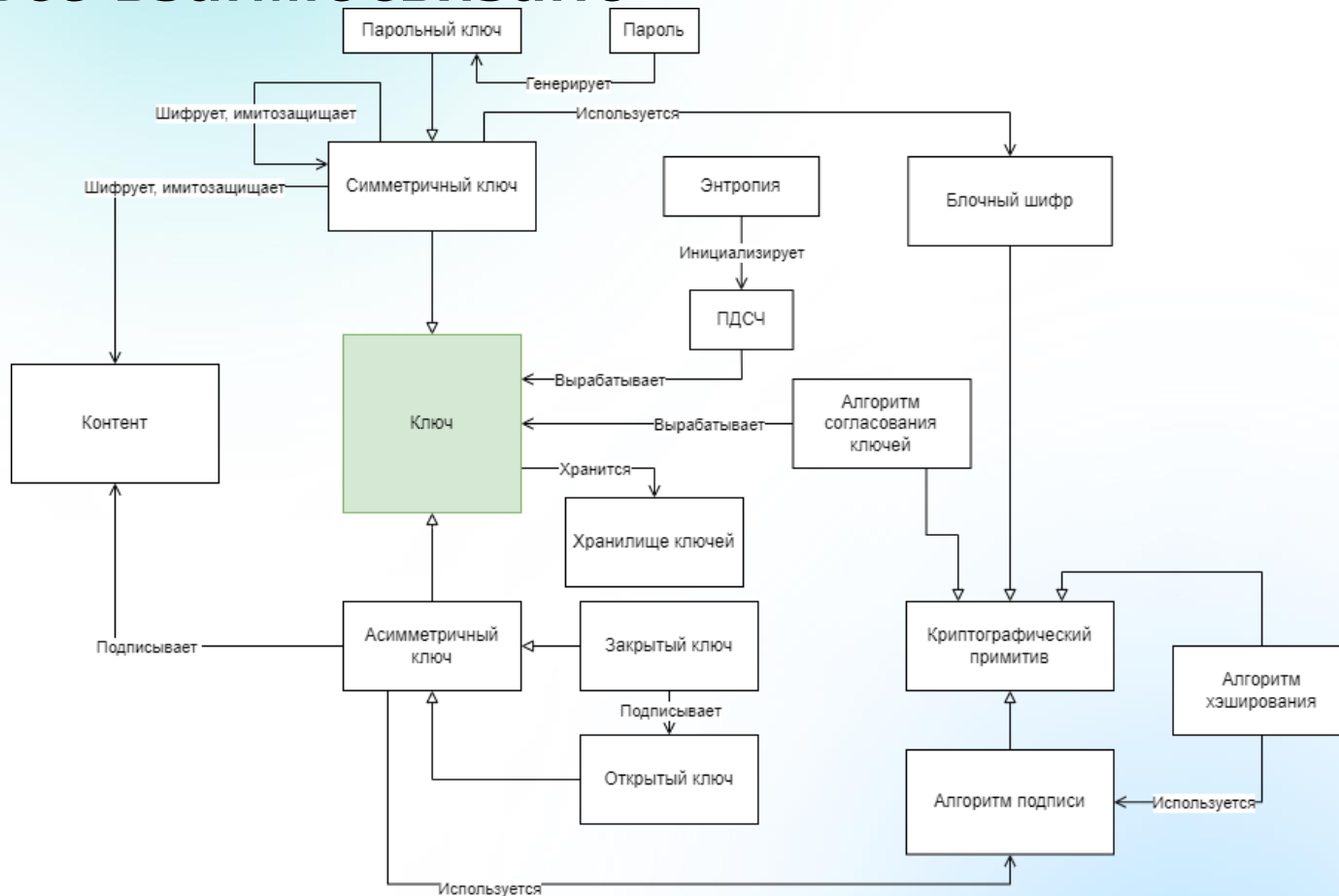
Бесключевая криптография



Выработка общего секрета

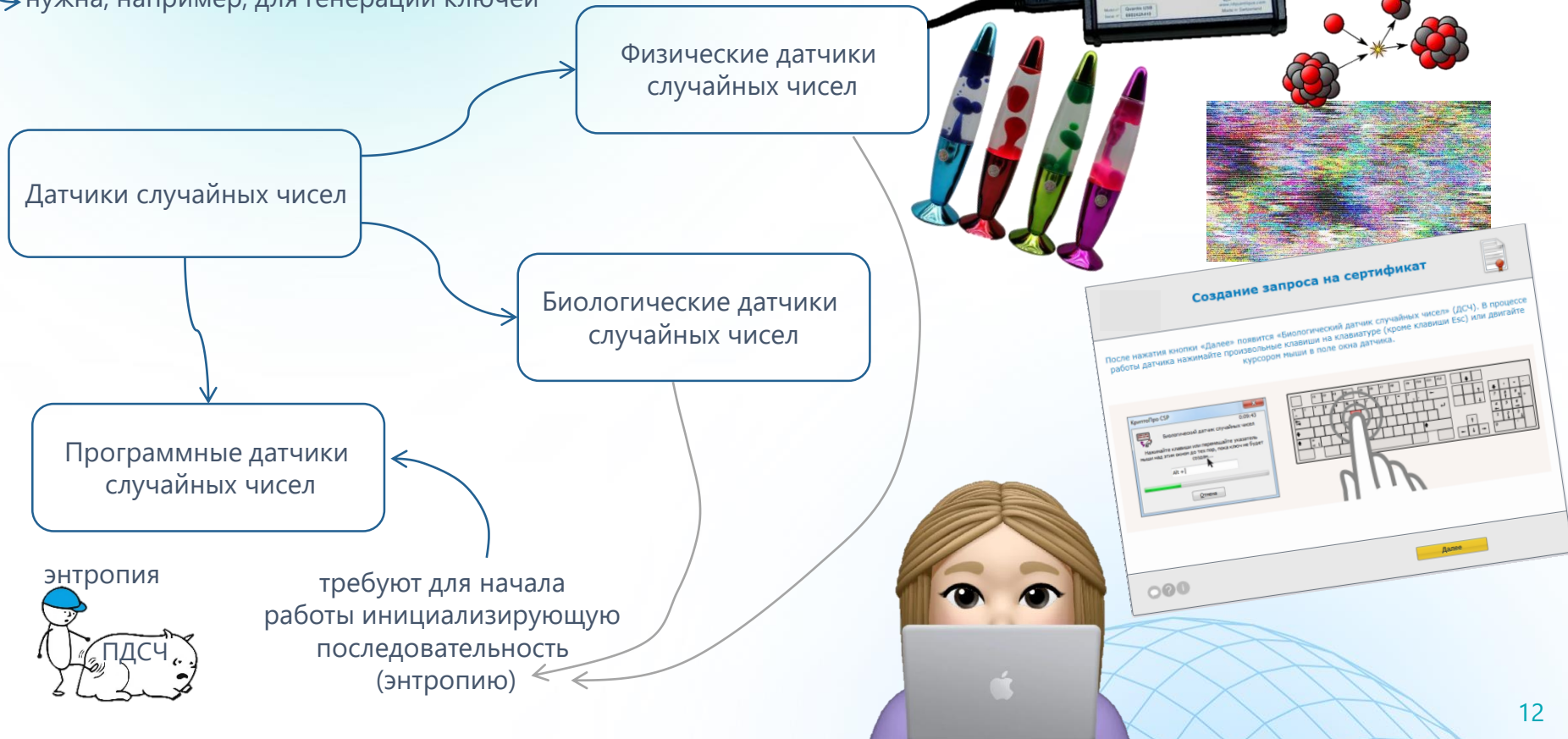


Как всё взаимосвязано

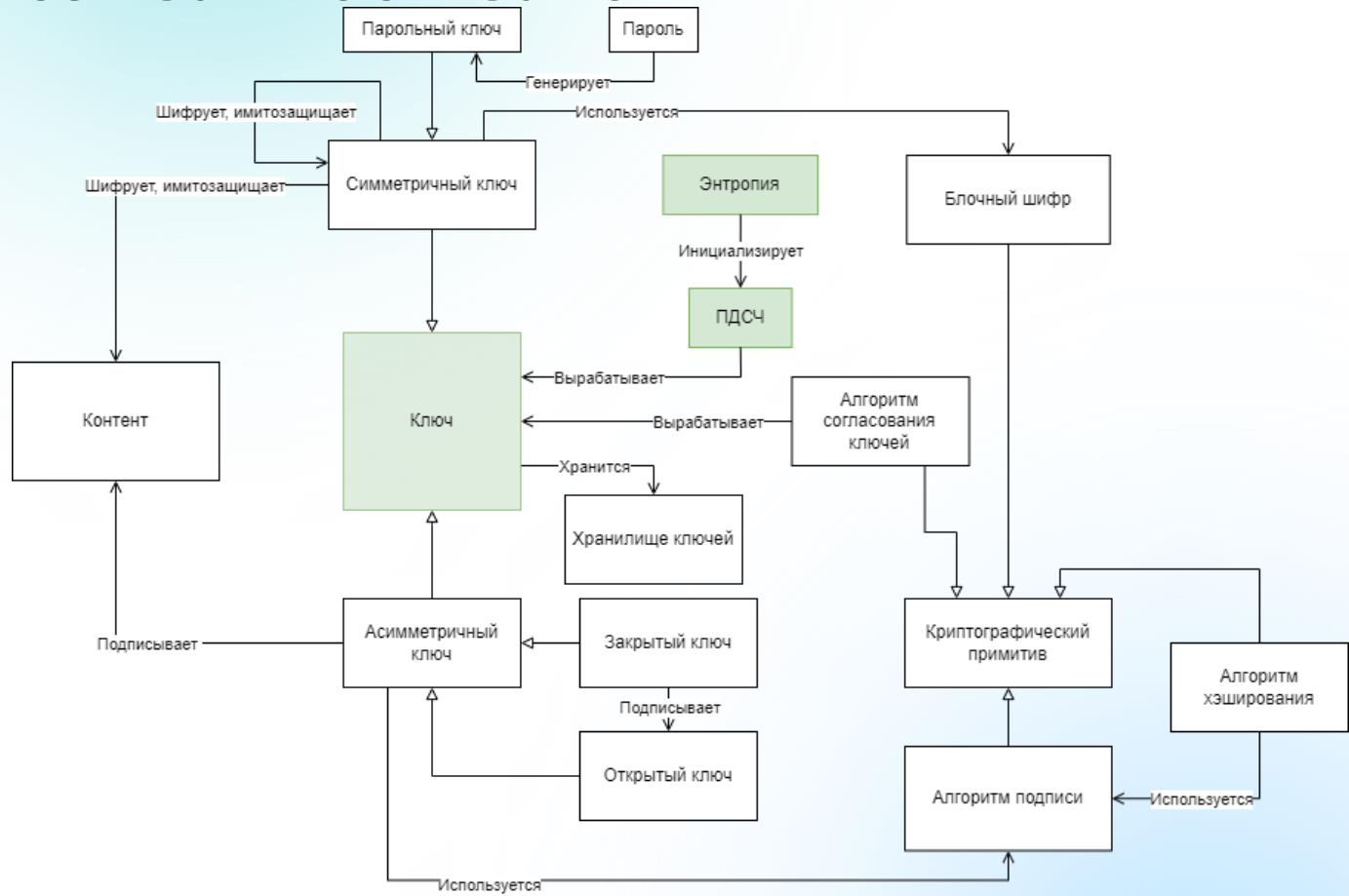


Случайность в криптографии

нужна, например, для генерации ключей



Как всё взаимосвязано



Ключи и их перемещения



Хранилища сертификатов в ОС и браузерах

- + автоматический поиск ключей приложениями
- + легко настроить
- специфичны для каждой ОС или браузера



транспорт

Файлы .pfx, .p12

- + универсальны
- + всегда защищены паролем
- ± легко распространить
- слабая защита, которая зависит от человека

Хранение ключей в долговременной памяти

- + удобно пользователю
- + удобно в разработке
- + связь с хранилищем сертификатов
- ключ может появиться в оперативной памяти

Токены и смарт-карты

- + повышенная безопасность
- + закрытый ключ не экспортируется
- привязка к вендору
- ограниченная производительность
- требуют СКЗИ каждому сотруднику

HSM

- + не нужны отдельные токены
- + поддержка легче, чем у токенов
- + использование ЭП во внутренних сценариях
- сложны в обслуживании



TPM и PUF

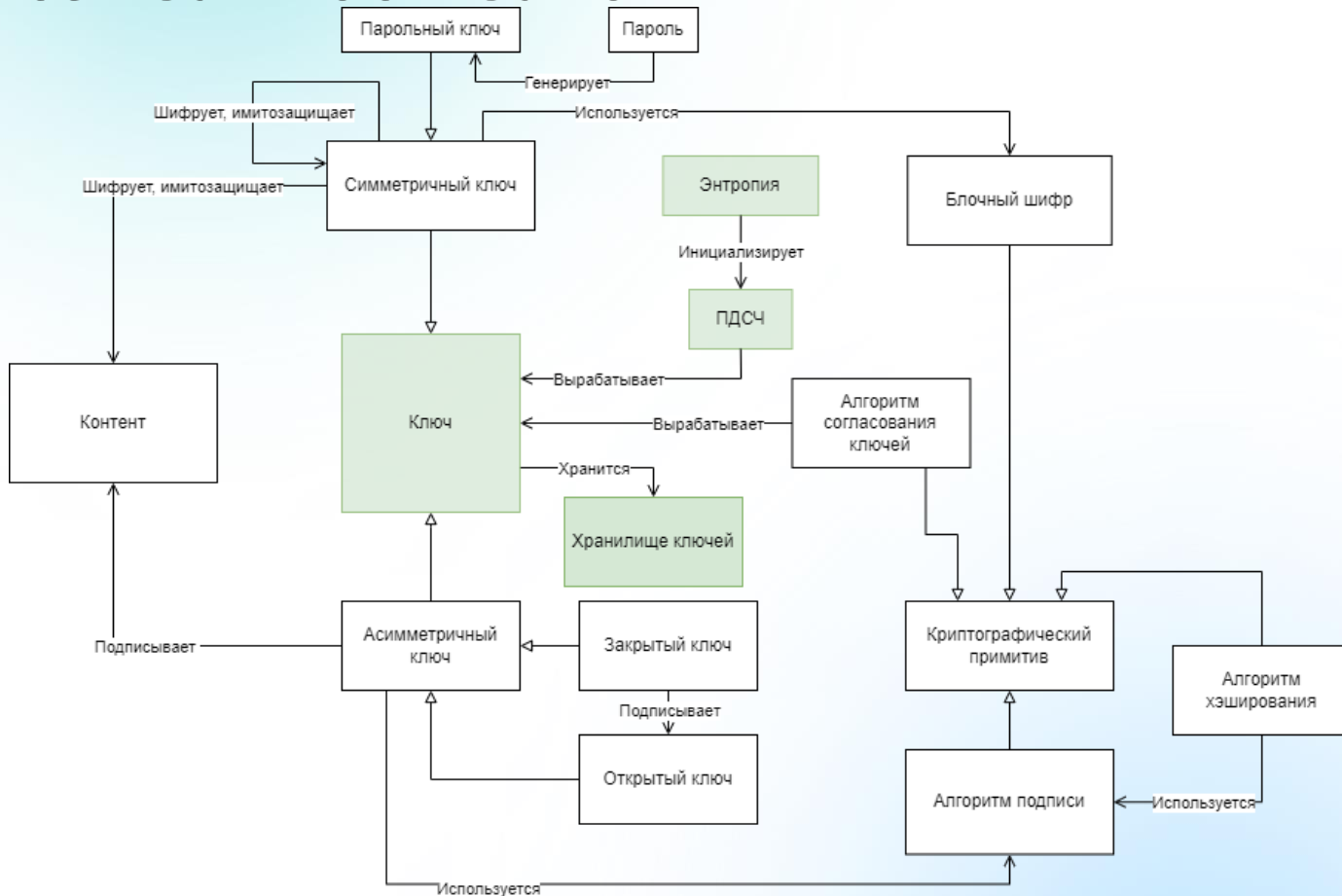
- + аппаратная защита ключей с помощью физических свойств
- реализация возможна только на устройствах, где есть необходимые компоненты



Физически неклонируемая функция — это функция, воплощённая в **физической** структуре, которую просто оценить, но трудно охарактеризовать, смоделировать или воспроизвести.



Как всё взаимосвязано

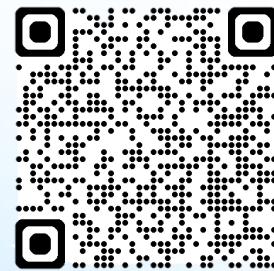


Реализация криптографии



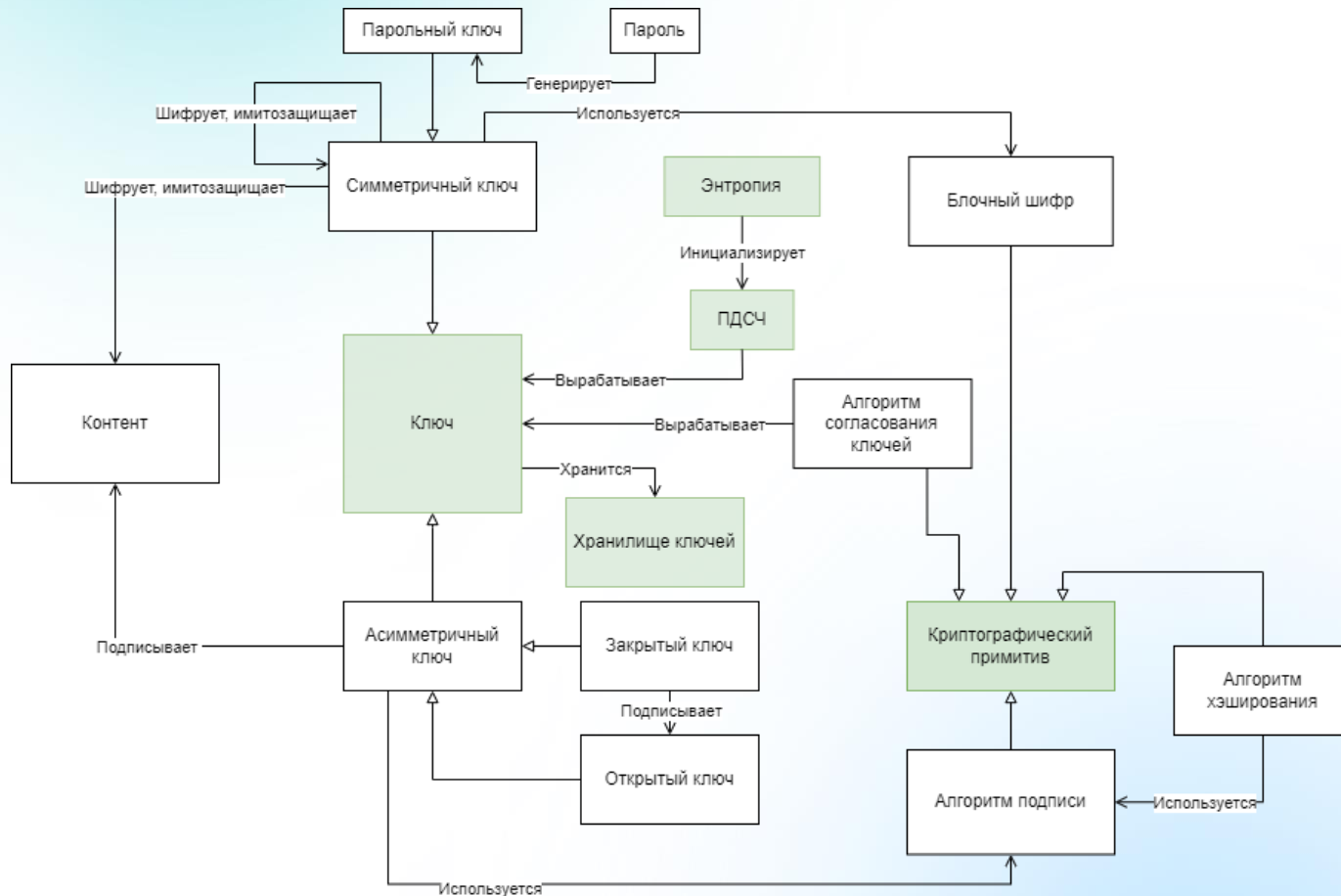
Уровень абстракции	Язык/Технология	Платформа	Решение
Функции низкого уровня: генерация ключей, шифрование, подпись	C++	Linux, Windows, macOS, Android, iOS	Botan
	Java, C#	JVM	Bouncy Castle
	C		PKCS#11 решение вендора, OpenSSL
Прикладные функции: формирование запросов и сертификатов, создание ЭП	PKCS#11 API, OpenSSL API	Linux, Windows, macOS, Android, iOS	PKCS#11 решение вендора, OpenSSL
	Microsoft Crypto API	Семейство Windows. Есть порт на GNU/Linux, OS X, iOS, Android	Криптопровайдеры под Windows: КриптоПро CSP, ViPNet CSP

Custom Algorithms
Don't do this.

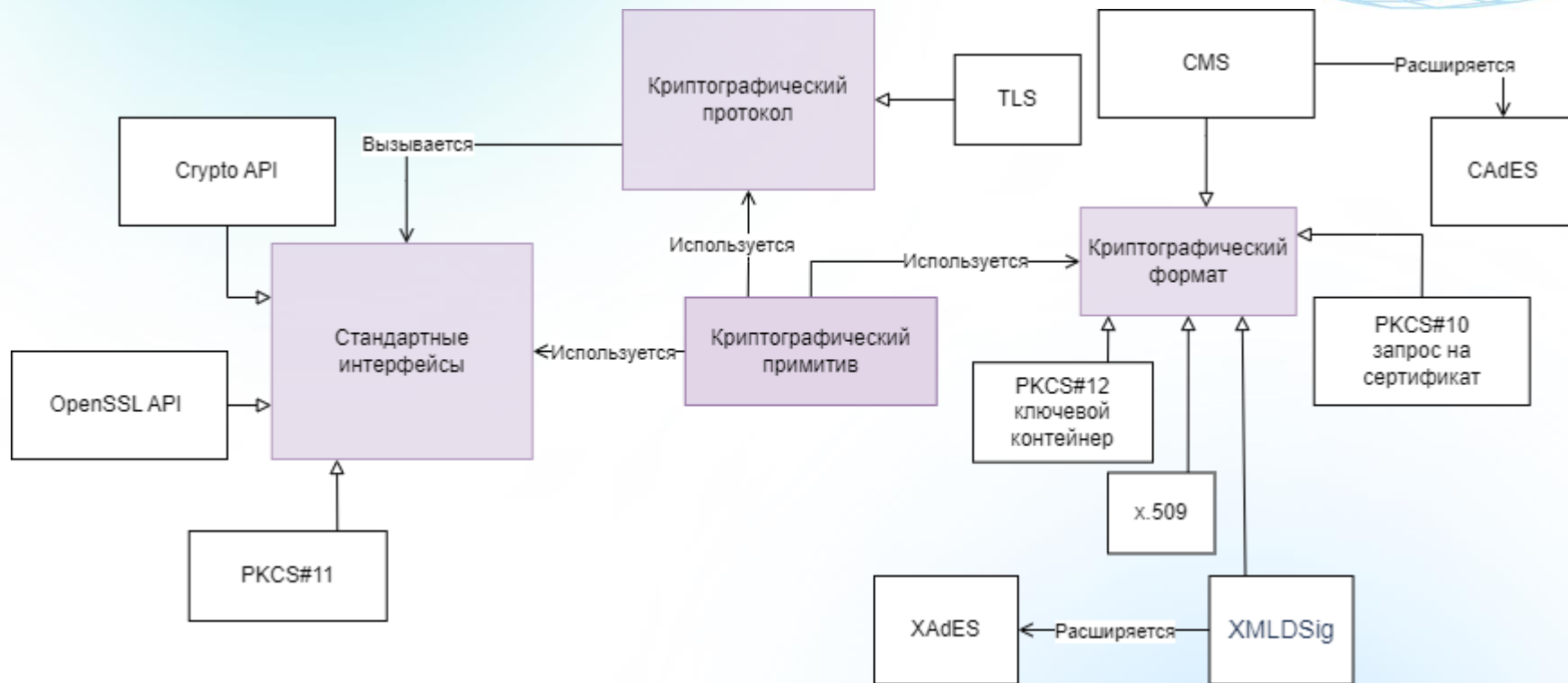


[Comparison of cryptography libraries](#)

Как всё взаимосвязано



Где это всё используется



Резюме – контрольная точка

Криптографические методы защиты информации		Базовые криптографические алгоритмы	Виды ключей	Ц	К	А	Н
Шифрование	Симметричное шифрование	•“Кузнечик” и “Магма” (ГОСТ Р 34.12--2015) •AES	Секретный ключ.				
	Асимметричное шифрование	•RSA	Закрытый ключ (ключ расшифрования), открытый ключ (ключ зашифрования).		+		
Электронная подпись (асимметричные схемы)		•ГОСТ Р 34.10--2012 •RSA •ECDSA •EdDSA	Закрытый ключ (ключ ЭП), открытый ключ (ключ проверки ЭП).	+		+	+
Хэширование		•“Стрибог” (ГОСТ Р 34.11--2012) •SHA-2 •SHA-3	Бесключевой криптографический механизм.	+			
Имитовставка		Те же, что и для симметричного шифрования и хэширования.	Ключ аутентичности.	+		+	

**А если ещё и сертифицировать
надо..?**

Сертификация криптографии в РФ

Р 1323565.1 010-2017

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО
СТАНДАРТИЗАЦИИ Р 1323565.
1.012.-2017

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Принципы разработки и модернизации
шифровальных (криптографических) средств
защиты информации

Издание официальное

Регистрировано в Минюсте РФ 3 марта 2005 г. № 6382

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ
от 9 февраля 2005 г. № 66

ОБ УТВЕРЖДЕНИИ ПОЛОЖЕНИЯ
О РАЗРАБОТКЕ, ПРОИЗВОДСТВЕ, РЕАЛИЗАЦИИ И ЭКСПЛУАТАЦИИ
ШИФРОВАЛЬНЫХ (КРИПТОГРАФИЧЕСКИХ) СРЕДСТВ ЗАЩИТЫ
ИНФОРМАЦИИ (ПОЛОЖЕНИЕ ПКЗ-2005)
(в ред. Приказа ФСБ РФ от 12.04.2010 № 173)

В целях определения порядка разработки, производства, реализации и эксплуатации шифровальных (криптографических) средств защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, приказываю:

1. Утвердить прилагаемое Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005).

2. Приказ ФАПСи от 23 сентября 1999 года № 158 (зарегистрирован Минюстом России 28 декабря 1999 года, регистрационный № 2029) не применять с даты вступления в силу настоящего Приказа.

Директор
Н.ПАТРУШЕВ



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.03.0001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер **СФ/124-0662** от **"18" мая 2021 г.**

Действителен до **"18" мая 2024 г.**

Выдан **Акционерному обществу «Информационные технологии и коммуникационные системы»**

Настоящий сертификат удостоверяет, что программный комплекс **VPN Client 4 (версия 4.3)** (обновления 1, 2, 3) в соответствии с требованиями **ФРКБ.00116-05.30.01-ФГО**

соответствует **Требованиям к средствам криптографической защиты информации, для защиты информации, не содержащей сведений, составляющих государственную тайну, классов КС1, КС2, КС3 для изменений 1, 2, 3, соответственно, режимов электронной подписи, утвержденных приказом ФСБ России от № 796, установленным для классов КС1, КС2, КС3 для изменений 1, 2, 3, может использоваться для криптографической защиты, создания и управления шифрами, файлами и данными, содержащимися в области государственной тайны, включенные в перечень для файлов и данных, содержащихся в ней, печати, в IP-трафике, вычисления значения хэш-функции для файлов и данных в области критической защиты, реализации функций электронной подписи с обеспечением анонимности от февраля 2011 г. № 63-ФЗ «Об электронной электронной подписи, проверки электронной подписки» информации, не содержащей сведений, составляющих государственную тайну.**

и на основании результатов производных **Общество с ограниченной ответственностью «Информационные технологии и коммуникационные системы»**

исполняет обязанности при использовании комплекса в соответствии с организационной документацией согласно формуляру **ФРКБ.00116-05.30.01-ФГО**.

Идентификационный номер **№ 782-001001**.

Информация обобщается при использовании комплекса в соответствии с организационной документацией согласно формуляру **ФРКБ.00116-05.30.01-ФГО**.

Идентификационный номер **№ 782-001001**.

Идентификационный номер **№ 782-001001**.

Идентификационный номер **№ 782-001001**.

Идентификационный номер **№ 782-001001**.

Идентификационный номер **№ 782-001001**.

Идентификационный номер **№ 782-001001**.

Идентификационный номер **№ 782-001001**.

Идентификационный номер **№ 782-001001**.

Идентификационный номер **№ 782-001001**.

Идентификационный номер **№ 782-001001**.

Идентификационный номер **№ 782-001001**.

Идентификационный номер **№ 782-001001**.

Идентификационный номер **№ 782-001001**.

Как разрабатывать ПО с криптографией внутри



Оценка влияния или сертификация?

Оценка влияния

Вызываются функции, описанные в правилах пользования **И** само встраиваемое СКЗИ сертифицировано



Лицензия на разработку защищенных с использованием шифровальных (криптографических) средств информационных систем



Результат
Заключение по оценке влияния

Создание нового СКЗИ

Вызываются функции, не описанные в правилах пользования, **или** встраиваемое СКЗИ не сертифицировано



Лицензия на разработку шифровальных (криптографических) средств



Результат
Сертификат соответствия

Криптография в мире

NIST



COMPUTER SECURITY

Номер RFC	Тема
RFC 768 (англ.) RFC 768 (рус.)	UDP
RFC 791 (англ.) RFC 791 (рус.)	IP
RFC 792 (англ.) RFC 792 Архивная копия от 7 ноября 2011 на Wayback Machine (рус.)	ICMP
RFC 793 (англ.) RFC 793 (рус.)	TCP



OWASP

®

infotecs

NIST Special Publication 800-108
**Recommendation for Key Derivation
Using Pseudorandom Functions**
(Revised)

Lily Chen

Computer Security Division
Information Technology Laboratory

October 2009



U.S. Department of Commerce
Gary Locke, Secretary
National Institute of Standards and Technology
Patrick Gallagher, Deputy Director

IEEE

Advancing Technology
for Humanity

Как проверить себя?

01.

Используемые алгоритмы

02.

Хранение секретов

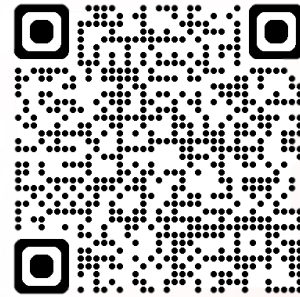
03.

Передача секретов

04.

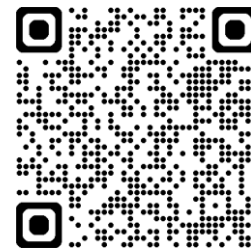
Случайные величины

[OWASP Developer
Guide | Principles of
Cryptography |
OWASP Foundation](#)



Чеклист: используемые алгоритмы

- Не использую нестандартизированные механизмы
 - Не использую устаревшие алгоритмы
 - Проверил актуальность алгоритма и не нашёл лучше
 - Проверил все требования заказчика
 - Размер ключей и выхода хэш-функции соответствует рекомендациям
 - Считаю имитовставку, потом зашифровываю
-
- Разрабатываемый продукт сохраняет необходимые (ожидаемые) функциональные характеристики при использовании криптографии



Encrypt-then-Sign или Sign-then-Encrypt, вот в чем вопрос

Чеклист: хранение секретов

Предусловие: выполнен чеклист 1

- Ключи **НЕ** хранятся в коде
- Ключи хранятся в защищённом виде:
 - На защищённом СКЗИ
 - На защищённом отчуждаемом ключевом носителе
 - ↓ В защищённом виде на диске
- У всех ключевых файлов R/O
- Изменения ключей регистрируются
- Хранилища ключей защищены с выполнением парольной политики

Чеклист: передача секретов

Предусловие: выполнены чеклисты 1 и 2

- Приватные ключи **НЕ** передаются в открытом виде }
 - приложение
 - протокол
 - сеть
- Я обоснованно использую уровень модели OSI при использовании криптографии
- Защита реализована близко к данным
- Ключи удаляются вовремя }
 - после использования
 - после закрытия сессии
 - после истечения срока действия
- Временные файлы безопасны
 - не сохраняю ли я где-то открытый текст?
 - не переношу ли я куда-то ключи в открытом виде?

Чеклист: случайные величины

Предусловие: отсутствует

- Пользуюсь рекомендованными функциями для генерации ключей
- Использую UUID из специальных программ
- Генерирую новые UUID для каждой новой сущности

UUIDGEN
API UuidCreate()

Language	Unsafe Functions	Cryptographically Secure Functions
C	<code>random(), rand()</code>	<code>getrandom(2)</code>
Java	<code>Math.random(), StrictMath.random(), java.util.Random, java.util.SplittableRandom, java.util.concurrent.ThreadLocalRandom</code>	<code>java.security.SecureRandom, java.util.UUID.randomUUID()</code>
PHP	<code>array_rand(), lcg_value(), mt_rand(), rand(), uniqid()</code>	<code>random_bytes(), Random\Engine\Secure in PHP 8, random_int() in PHP 7, openssl_random_pseudo_bytes() in PHP 5</code>
.NET/C#	<code>Random()</code>	<code>RandomNumberGenerator</code>



Выводы

не нужно её бояться!!

1. Криптография – это матрёшка
2. Отталкивайтесь от задач и уровня абстракции
3. Читайте и уточняйте тз!!
4. Проверяйте себя по пунктам чек-листа

нормально делай
нормально будет



Полезные материалы



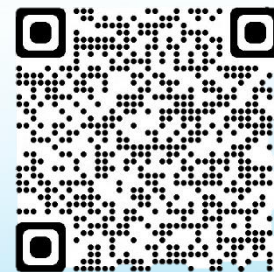
**Н. СМАРТ
«Криптография»**



**Б. Шнайер «Прикладная
криптография. Протоколы,
алгоритмы, исходные тексты на
языке Си»**

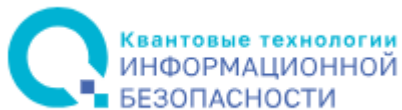


**Владимир Иванов
«Криптография,
шифрование»**



Если хотите посмотреть на науку

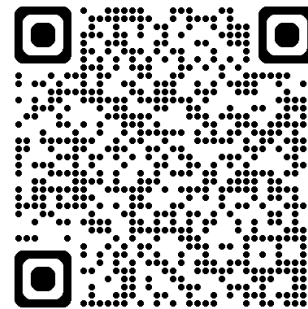
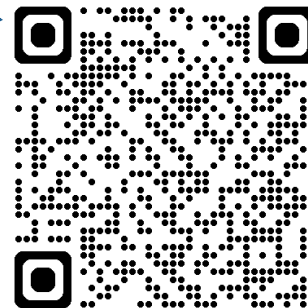
Квантовые технологии для защиты информации (quantum-crypto.ru)



Справочная: квантовая криптография на пальцах



База знаний.
Постквантовая криптография





Ответы на вопросы

Спасибо за внимание!

infotecs.ru



Карьера



infotecs.team

