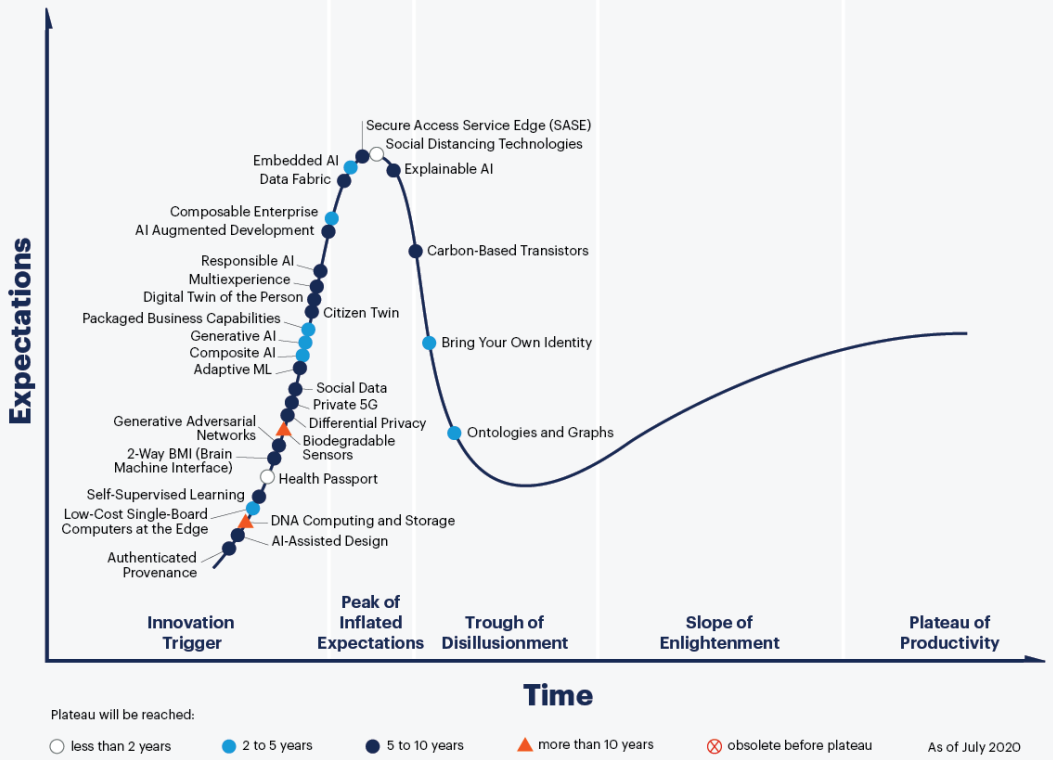
Ежегодная международная научно-практическая конференция
«РусКрипто’2021»

Требования к средствам криптографической защиты информации, предназначенным для обеспечения защиты новых информационных технологий

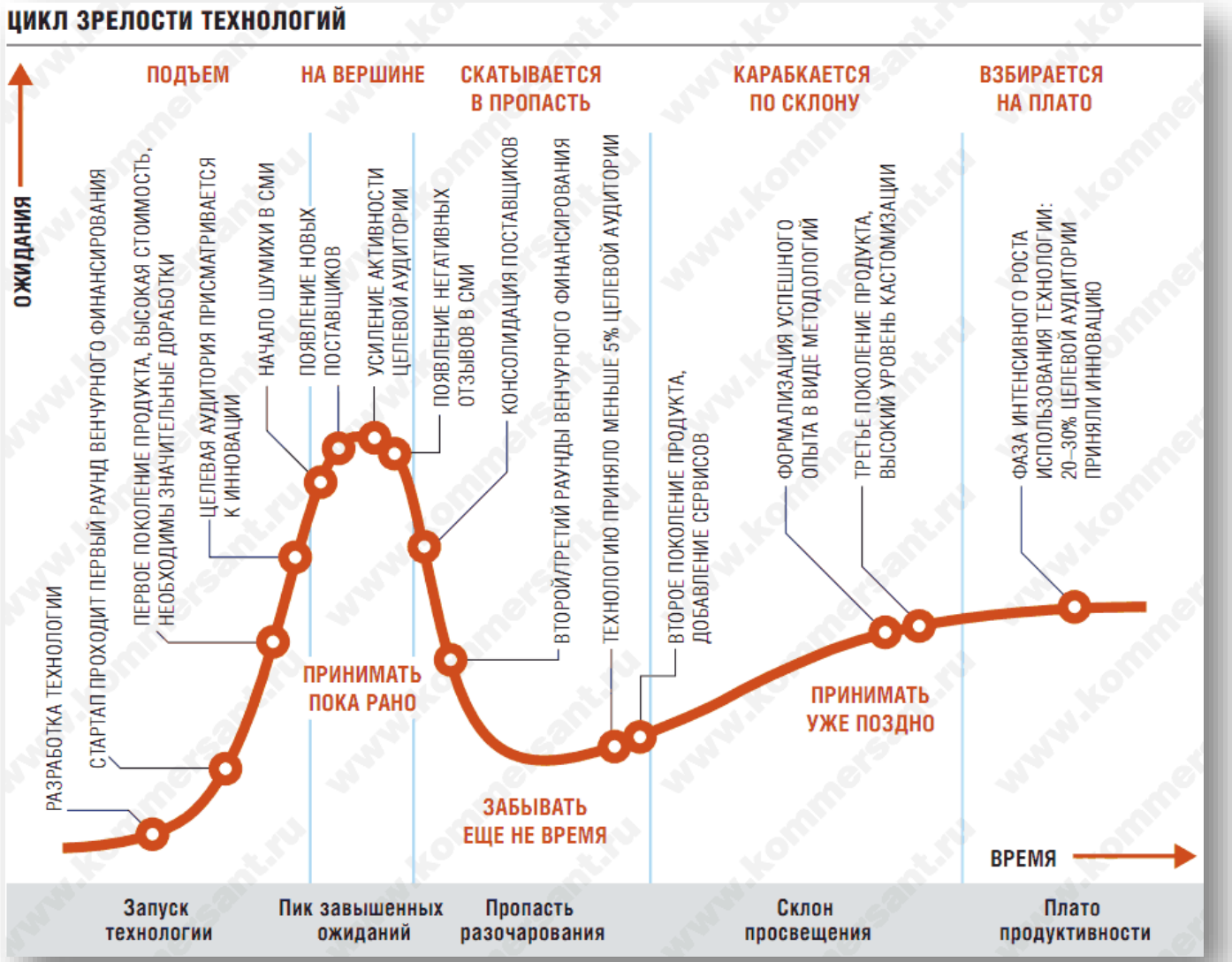
Толстолуцкая Анастасия

Hype Cycle for Emerging Technologies, 2020



gartner.com/SmarterWithGartner

Gartner


ЦИКЛ ЗРЕЛОСТИ ТЕХНОЛОГИЙ
ПОДЪЕМ
НА ВЕРШИНЕ
СКАТЫВАЕТСЯ В ПРОПАСТЬ
КАРАБКАЕТСЯ ПО СКЛОНУ
ВЗБИРАЕТСЯ НА ПЛАТО
ОЖИДАНИЯ
РАЗРАБОТКА ТЕХНОЛОГИИ
СТАРТАП ПРОХОДИТ ПЕРВЫЙ РАУНД ВЕНЧУРНОГО ФИНАНСИРОВАНИЯ
ПЕРВОЕ ПОКОЛЕНИЕ ПРОДУКТА, ВЫСОКАЯ СТОИМОСТЬ, НЕОБХОДИМЫ ЗНАЧИТЕЛЬНЫЕ ДОРАБОТКИ
ЦЕЛЕВАЯ АУДИТОРИЯ ПРИСМАТРИВАЕТСЯ К ИННОВАЦИИ
НАЧАЛО ШУМИХИ В СМИ
ПОЯВЛЕНИЕ НОВЫХ ПОСТАВЩИКОВ
УСИЛЕНИЕ АКТИВНОСТИ ЦЕЛЕВОЙ АУДИТОРИИ
ПОЯВЛЕНИЕ НЕГАТИВНЫХ ОТЗЫВОВ В СМИ
КОНСОЛИДАЦИЯ ПОСТАВЩИКОВ
ВТОРОЙ/ТРЕТИЙ РАУНДЫ ВЕНЧУРНОГО ФИНАНСИРОВАНИЯ
ТЕХНОЛОГИЮ ПРИНЯЛО МЕНЬШЕ 5% ЦЕЛЕВОЙ АУДИТОРИИ
ВТОРОЕ ПОКОЛЕНИЕ ПРОДУКТА, ДОБАВЛЕНИЕ СЕРВИСОВ
ФОРМАЛИЗАЦИЯ УСПЕШНОГО ОПЫТА В ВИДЕ МЕТОДОЛОГИЙ
ТРЕТЬЕ ПОКОЛЕНИЕ ПРОДУКТА, ВЫСОКИЙ УРОВЕНЬ КАСТОМИЗАЦИИ
ФАЗА ИНТЕНСИВНОГО РОСТА ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИИ: 20–30% ЦЕЛЕВОЙ АУДИТОРИИ ПРИНЯЛИ ИННОВАЦИЮ
ПРИНИМАТЬ ПОКА РАНО
ЗАБЫВАТЬ ЕЩЕ НЕ ВРЕМЯ
ПРИНИМАТЬ УЖЕ ПОЗДНО
ВРЕМЯ
Запуск технологии
Пик завышенных ожиданий
Пропасть разочарования
Склон просвещения
Плато продуктивности

- Блокчейн
- Квантовые технологии
- Искусственный интеллект
- «Интернет вещей»

Блокчейн

Соответствие блокчейн-решений требованиям ФСБ России:

- в случаях, когда применение Положение ПКЗ-2005 является обязательным;
- в случаях, когда разработка блокчейн-решений производится в рамках работ по созданию государственных информационных систем.

Применение технологии блокчейн

- Банки и финансовые услуги
  - «Цифровые банковские гарантии»
  - «Децентрализованная депозитарная система для учета закладных»
  - Пилотные проекты учетных систем грузоперевозок
- Государственный сектор
- Энергетика
- Образование

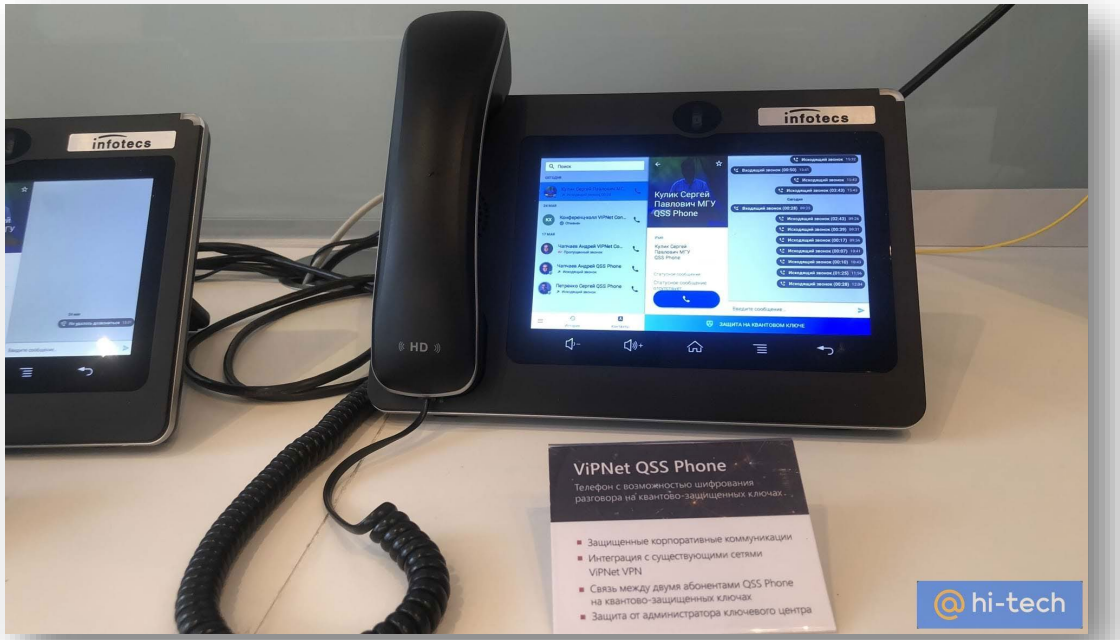
Квантовые технологии

Временные требования к квантовым криптографическим системам выработки и распределения ключей для средств криптографической защиты информации, не содержащей сведений, составляющих государственную тайну, определяют:

- терминологию в области ККС ВРК;
- классификацию систем ККС ВРК, в привязке к существующей классификации средств криптографической защиты информации (СКЗИ);
- описание базовых возможностей нарушителя в отношении ККС ВРК различных классов;
- критерий криптографической стойкости ключей, вырабатываемых ККС ВРК, а также предельно допустимую границу данного критерия;
- требования к аппаратно-программной реализации ККС ВРК;
- инженерно-криптографические, специальные и иные требования по информационной безопасности ККС ВРК, аналогичные требованиям, предъявляемым к классическим СКЗИ.

Применение квантовых технологий

Разработка компании АО «ИнфоТеКС» и Центра квантовых технологий МГУ первого в России телефона с квантовой защитой связи (ViPNet QSS Phone).



Применение квантовых технологий

- Построение квантовых сетей в РЖД

Искусственный интеллект

Атаки, специфичные для систем машинного обучения

- Атаки на процесс обучения - направлены на изменение последующей логики функционирования системы за счет подачи на вход специальным образом сформированных данных.
- Атаки на этапе работы.
- Атаки, нарушающие конфиденциальность данных, использованных при обучении нейронных сетей.

Методы защиты алгоритмов машинного обучения:

- Статистическое обезличивание
- Гомоморфное шифрование
- Протоколы распределенных безопасных вычислений

Теоретические и практические вопросы построения защищенных систем искусственного интеллекта включены в федеральный проект «Искусственный интеллект».

«Интернет вещей»

17 сентября 2019 года в Российской Федерации утверждены «Требований к средствам криптографической защиты информации, предназначенным для обеспечения некорректируемой регистрации информации, не содержащей сведений, составляющих государственную тайну» (СКЗИ-НР).

Под некорректируемой регистрацией информации понимается такой способ обработки информации средством регистрации, по результатам которой обеспечивается:

- регистрация информации в соответствии с установленным перечнем;
- идентичность зарегистрированной информации с информацией, предназначенной для регистрации (формирования и(или) записи), хранения и(или) передачи;
- непрерывность регистрации (защита от нарушения последовательности регистрации блоков информации);
- возможность гарантированного выявления фактов ее корректировки или фальсификации по результатам проверки, в том числе и фактов нарушения последовательности зарегистрированных событий (непрерывности регистрации);
- возможность гарантированной аутентификации средства регистрации.

СКЗИ-НР представляет собой аппаратно-программное шифровальное (криптографическое) средство в опломбированном корпусе, применяющееся для нейтрализации целенаправленных действий нарушителя, совершаемых с целью создания условий, при которых возможен перевод средства регистрации в такой режим работы, при котором нарушается режим обеспечения некорректируемой регистрации информации данным средством.

Общие требования к СКЗИ-НР

- Обеспечение некорректируемой регистрации информации средством регистрации, функционирующим совместно с СКЗИ-НР.
- Все криптографические протоколы (алгоритмы, функции) должны реализовываться в среде специальных аппаратных средств СКЗИ-НР.
- Должен быть реализован форматно-логический контроль информации, передаваемой в СКЗИ-НР из средства регистрации, совместно с которым эксплуатируется СКЗИ-НР.
- Должна быть реализована блокировка СКЗИ-НР при подаче на вход информации, воспринимаемой СКЗИ-НР как свидетельствующей о нарушении режима штатного функционирования средства регистрации, совместно с которым эксплуатируется СКЗИ-НР (критическая информация).

Необходимые условия:

- контролирующие органы имеют возможность проверить криптографического проверочного кода, сформированный любым экземпляром СКЗИ-НР;
- компрометация криптоключей одного экземпляра СКЗИ-НР не приводит к компрометации криптоключей других экземпляров СКЗИ-НР;
- механизм проверки криптографического проверочного кода исключает возможность компрометации ключа формирования криптографического проверочного кода с учетом конкретизированной модели нарушителя и угроз для конкретной системы обеспечения некорректируемой регистрации информации.

Совокупность аппаратно-программных систем защиты, которые должны реализовывать в себе специальные аппаратные средства СКЗИ-НР :

- активный защитный экран (сетка), обеспечивающий защиту от физического проникновения к логическим элементам, защиту от оптического зондирования (анализа топологии) и контроля целостности путем пропускания по шинам защитного экрана произвольных неповторяющихся последовательностей;
- система защиты по цепям питания, обеспечивающая невозможность функционирования специальных АС СКЗИ-НР при нахождении питающих напряжений в недопустимых пределах;
- система защиты по цепям питания, осуществляющая аппаратное выравнивание/зашумление профиля энергопотребления;
- система поиска ошибок, реализующая функции выявления несанкционированных изменений данных в памяти;
- модуль защиты памяти (MPU) в части разграничения прав доступа к различным областям памяти со стороны пользователей и приложений;
- датчик света, противодействующий оптическим атакам на критические цифровые узлы схемы;
- внутренний тактовый генератор с переменной частотой тактирования произвольным рандомизированным образом (без предъявлений требований к закону распределения, в диапазоне частот не хуже fтакт ±5%);
- система защиты от утечки по ТКУИ.

Применение

- значимые системы контрольно-кассовой техники;
- значимые системы тахографического контроля;
- промышленные счетчики и датчики.

Выводы:

- Блокчейн - для данной технологии нет необходимости вводить специальные требования.
- Квантовые технологии - утверждены «Временные требования к квантовым криптографическим системам выработки и распределения ключей для средств криптографической защиты информации, не содержащей сведений, составляющих государственную тайну».
- Искусственный интеллект - нет требований по информационной безопасности.
- «Интернет вещей» - утверждены «Требования к средствам криптографической защиты информации, предназначенным для обеспечения некорректируемой регистрации информации, не содержащей сведений, составляющих государственную тайну».

Спасибо за внимание!

Список использованных источников

- https://www.gartner.com/smarterwithgartner/5-trends-drive-the-gartner-hype-cycle-for-emerging-technologies-2020/
- Елистратов А., Маршалко Г., Светушкин В. Подводные камни сертификации блокчейн-решений. // Открытые системы. СУБД [Электронный ресурс]. - 2019. - № 1. - С. 21-23.
- http://www.fsb.ru/fsb/science/single.htm%21id%3D10437338%40fsbResearchart.html
- Ушаков Денис Сергеевич, Подольская Татьяна Валентиновна, Сысоева Анна Андреевна Анализ потенциала применения блокчейн-технологии в современной мировой экономике // Государственное и муниципальное управление. Ученые записки. 2019. №1. URL: https://cyberleninka.ru/article/n/analiz-potentsiala-primeneniya-blokcheyn-tehnologii-v-sovremennoy-mirovoy-ekonomike.