XXIX научно-практическая конференция
«КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ»

infotecs

Технологическая независимость и усиление ИБ.

Обзор нормативной базы

Сергей Акимов
Заместитель генерального директора АО «ИнфоТеКС»

Участники:

- Президент
- Правительство
- ФСБ России
- ФСТЭК России
- Минцифры (в частности Роскомнадзор)
- Центральный банк
- Отраслевые министерства и ведомства
- Технические комитеты
  (в частности ТК №26, ТК №362, ТК №122,
  ТК №167«ПАК для КИИ и ПО для них»)

Направления деятельности:

- КИИ
- ГосСОПКА
- ПДн
- ГИС
- Защита ГТ и КИ
- Лицензирование и сертификация
- Ведение Реестров
  (Российского ПО, ЕРРРП, ТОРП)
- Доверенные ПАКи
- Квантовое распределение ключей

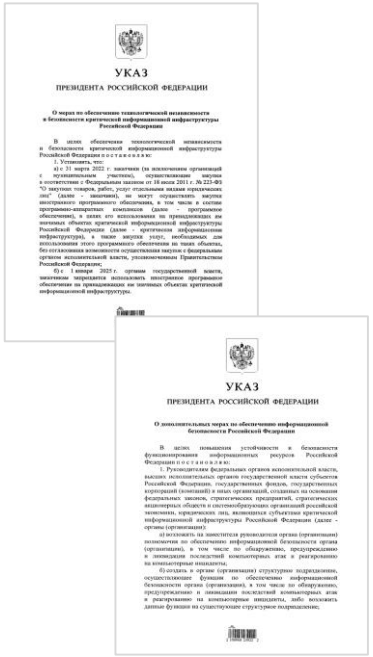
Значимые события 2023 года в области ИБ

1. Технологическая независимость и усиление ИБ
2. Об ответственности компаний, работающих с ПДн
3. Цифровой рубль. Первые шаги
4. Концепция регулирования отрасли квантовых коммуникаций
5. Искусственный интеллект

Технологическая независимость и усиление ИБ. Указы Президента

1) **Указ Президента РФ от 30 марта 2022 г. №166**
   «О мерах по обеспечению технологической независимости и безопасности КИИ РФ»

2) **Указ Президента РФ от 1 мая 2022 г. №250**
   «О дополнительных мерах по обеспечению ИБ РФ»


УКАЗ
ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

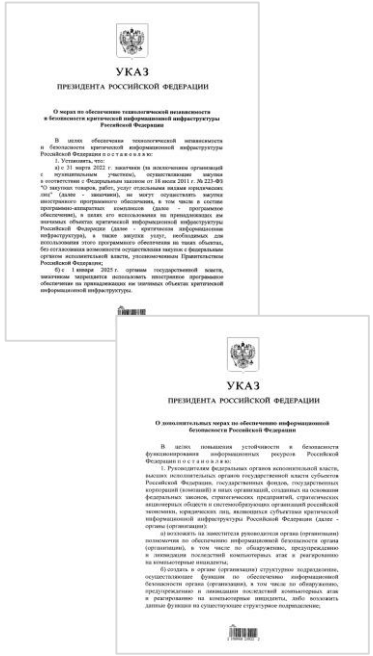
О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации

УКАЗ
ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

О дополнительных мерах по обеспечению информационной безопасности Российской Федерации

2024 год. Технологическая независимость и усиление ИБ. Реализация указов Президента

- **С 31 марта закупка иностранного ПО для ЗО КИИ только по согласованию** с уполномоченным ФОИВом
- **С 1 января 2025 г. ЗАПРЕЩАЕТСЯ ИСПОЛЬЗОВАТЬ ИНОСТРАННОЕ ПО на значимых объектах КИИ**
- Преимущественное **применение ДОВЕРЕННЫХ ПАК на ЗО КИИ**
- **С 1 января 2025 г. органам ЗАПРЕЩАЕТСЯ ИСПОЛЬЗОВАТЬ СЗИ производителей из недружественных стран**
- **Введена персональная ответственность руководителей за состояние ИБ**
- **Обязательно создание структурного подразделения ИБ**
- Проведение дополнительных мероприятий по линии функционирования НКЦИ, ГосСОПКИ


УКАЗ
ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

Только российские (сертифицированные) средства защиты

Приказ ФСБ России от 24 октября 2022 г. №524 «Об утверждении Требований о защите информации, содержащейся в ГИС, с использованием шифровальных (криптографических) средств»

Указание Банка России от 18 февраля 2022 г. №6071-У
фактический **запрет на широкое использование ПЭП** для подтверждения транзакций в финансовых операциях с переходом на УНЭП, или УКЭП, или СКЗИ с функцией имитозащиты

Требования по обеспечению безопасности ЗО КИИ РФ, действующие с 1 января 2023 г.
(в соответствии с Приказом ФСТЭК России от 20 февраля 2020 г. №35.)

- **СЗИ должны соответствовать** 6 или более высокому уровню доверия
- **Прикладное ПО,** планируемое к внедрению **должно соответствовать**:
  - Требованиям по безопасной разработке ПО
  - Требованиям к испытаниям по выявлению уязвимостей в ПО
  - Требованиям к поддержке безопасности ПО

Прекращение действия сертификатов соответствия на СЗИ

Изменение требований по безопасности информации

Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий

утверждены приказом ФСТЭК России от 2 июня 2020 г. № 76

Приказ зарегистрирован Минюстом России 11 сентября 2020 г. № 59772

Приказы ФСТЭК России от 31 марта 2022 г. № 61 от 15 апреля 2022 г. № 66 от 15 апреля 2022 г. № 67

1. Система корпоративного мобильного рабочего места WorksPad.
2. ПК DeviceLock 8 DLP Suite.
3. ПАК Коммутатор Huawei серии S5720».
4. ПАК ViPNet xFirewall 4
5. СЗИ «Secret Net LSP - C»

……

37. ПО OpenText Documentum 16.4.

Прекращение технической поддержки сертифицированных средств защиты информации

Перечень иностранных государств и территорий, совершающих недружественные действия в отношении Российской Федерации, российских юридических и физических лиц

утвержден распоряжением Правительства Российской Федерации от 5 марта 2022 г. № 430-р

Приказы ФСТЭК России от 12 мая 2022 г. № 85, от 12 июля № 123 от 18 августа 2022 г. №150

1. ОС SUSE Linux Enterprise Server 12 SP3
2. ПО «SAP Application Platform 7»
3. ПАК «FortiGate», функционирующий под управлением ОС FortiOS версии 6.X
4. ОС Red Hat Enterprise Linux 8
5. ПК VMware vSphere with Operations Management 6

……

40. ОС Microsoft Windows 10 в редакции Корпоративная

(Использован слайд из доклада Д.Н.Шевцова от 31.08.2022)

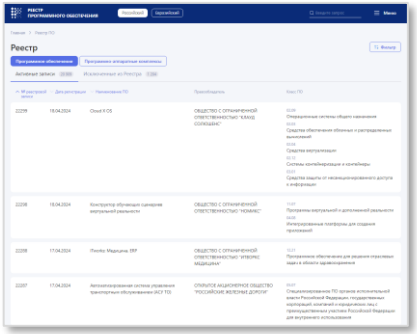
Изменения в реестрах Минцифры и Минпромторга

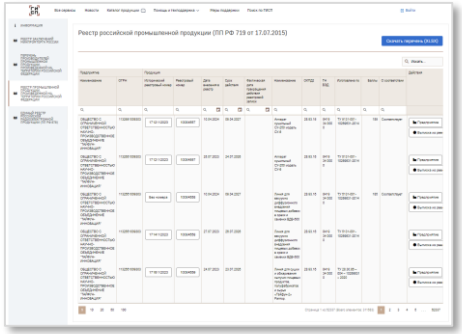
Реестры Минцифры

- **Введен дополнительный раздел – Программно-аппаратные комплексы** (ПАКи)
  В раздел ПАК уже включены: ViPNet Клиентский узел квантовой сети Лайт, ViPNet Распределительный узел квантовой сети Лайт, ViPNet Coordinator HW 4 (всего 7 исполнений)
- **Готовятся изменения в ПП от 23.03.2017 г. №325**
  «Об утверждении дополнительных требований к программам для ЭВМ и БД, сведения о которых включены в реестр российского ПО…»
  Почтовые приложения, средства видеоконференцсвязи, мессенджеры должны обеспечивать интеграцию с сертифицированными российскими СКЗИ в целях обеспечения конфиденциальности передаваемой информации

Реестр Минпромторга радиоэлектронной продукции

- **Готовятся изменения в ПП от 17.06.205 г. №719**
  вводится бальная система оценки с рядом обязательных требований





Переход субъектов КИИ на доверенные ПАКи

Указ Президента РФ от 30 марта 2022 г. № 166
«О мерах по обеспечению технологической независимости и безопасности……»

- «… определить сроки и порядок перехода субъектов КИИ на преимущественное применение доверенных программно-аппаратных комплексов …»

ПП РФ от 14.11.2023 № 1912
«О порядке перехода субъектов КИИ РФ на преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им значимых объектах КИИ РФ»

- **Переход** на преимущественное применение доверенных ПАК на ЗОКИИ **осуществляется до 1 января 2030 г.**
- **С 1 сентября 2024 г. не допускается использование ПАК, приобретенных с 1 сентября 2024 г. и не являющихся доверенными ПАК-ми** (за исключением случаев отсутствия аналогов)
- **Определены ФОИВ, ответственные за организацию перехода** субъектов КИИ РФ на преимущественное применение доверенных ПАК на принадлежащих им ЗО КИИ РФ
- **Утверждены Правила перехода** субъектов КИИ РФ на преимущественное применение доверенных ПАК на принадлежащих им ЗО КИИ РФ
- **До 1 сентября 2024 г. уполномоченные ФОИВ должны утвердить планы** организации перехода субъектов КИИ РФ на преимущественное применение доверенных ПАК

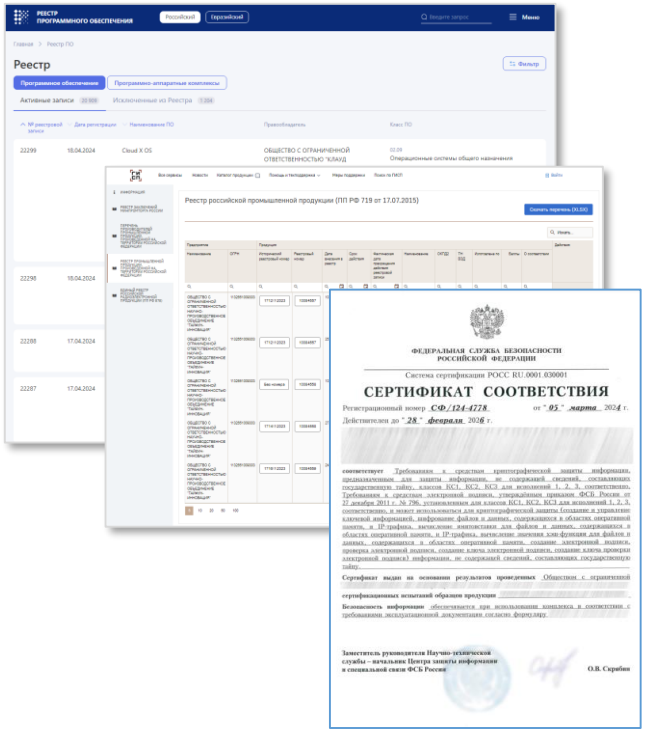
Доверенные ПАКи

В соответствии с ПП №1912 ПАК ИБ является доверенным, если:

1. Сведения о ПАК содержатся в реестре РЭП (МПТ)

2. ПО, используемое в составе ПАК, включено в реестр российского ПО (Минцифры)

3. ПАК сертифицирован ФСБ России и (или) ФСТЭК России



ФСТЭК России. Развитие системы сертификации СЗИ

- **Совершенствование требований по безопасности информации к СЗИ**
  - **Требования по безопасности информации к NGFW** (приказ ФСТЭК России от 07.04.2022 г. № 44)
  - **Требования по безопасности информации к системам управления базами данных** (приказ ФСТЭК России от 14.04.2023 г. № 64)
- **Повышение уровня квалификации Экспертов**
  - **Порядок аттестации экспертов органов по сертификации и испытательных лабораторий**
    Вступает в силу 01.09.2024 г. (приказ ФСТЭК России от 27.07.2023 г. № 147)
- **Создание инфраструктуры тестирования (планируется)**
  - **Создание Центра компетенций по тестированию производительности,** устойчивости функционирования и функциональных возможностей МЭ и иных сетевых устройств
  - **Создание среды тестирования СЗИ** путем эмуляции действий нарушителей безопасности информации и обеспечения её функционирования
  - **Методика тестирования производительности NGFW** (подготовлен проект)

Требования к многофункциональным МЭ

Многофункциональный межсетевой экран уровня сети – **программно-аппаратное средство, реализующее контроль за информацией и обеспечивающее защиту информационной (автоматизированной) системы от угроз безопасности информации, связанных с подключением к сетям связи общего пользования**

Предъявляются требования к:

- Обнаружению и блокированию компьютерных атак
- Обнаружению и блокированию вредоносного ПО
- Доверенной загрузке МЭ (с применением сертифицированного СДЗ)
- Производительности МЭ (должны быть зафиксированы сведения о пропускной способности, подтвержденные методикой)
- Применению сертифицированных СКЗИ
- Аппаратной фильтрации ……

ФСТЭК России подготовлен проект
Методики тестирования производительности многофункционального МЭ уровня сети

В 2025 году планируется создание
Центра компетенций по тестированию производительности, устойчивости функционирования и функциональных возможностей МЭ и иных сетевых устройств, реализующих функции безопасности информации

ФСТЭК России. Безопасная разработка программного обеспечения

Приказ ФСТЭК России от 01.12.2023 №240
«Об утверждении Порядка сертификации процессов безопасной разработки ПО СЗИ»
Порядок вступает в силу с 01.06.2024 г.

Стандарты по безопасной разработке

Введены в действие с 01.04.2024 г.:

- ГОСТ Р 71206-2024 «Защита информации. **Разработка безопасного программного обеспечения. Безопасный компилятор языков С/С++.** Общие требования»
- ГОСТ Р 71207-2024 «Защита информации. **Разработка безопасного программного обеспечения. Статический анализ программного обеспечения.** Общие требования»

Планируются к утверждению в 2024 г.:

- ГОСТ Р 56939 «Защита информации. **Разработка безопасного программного обеспечения. Общие требования**» (пересмотр ГОСТ Р 56939-2016. Подготовлена окончательная редакция)
- ГОСТ Р «Защита информации. **Разработка безопасного программного обеспечения. Композиционный анализ программного обеспечения.** Общие требования»
- …

ФСТЭК России. Повышение безопасности системного ПО

Центр исследования безопасности системного программного обеспечения:

- **Технологический центр исследования безопасности ядра Linux**
  (313 патчей разработано и принято)
- **Технологический центр исследования безопасности критичных компонентов**
  (47 патчей разработано и принято)

Консорциум участников по поддержке Центра исследования

(включает более 30 организаций, разрабатывающих сертифицированные решения на основе ядра)

Мероприятие национального проекта «Экономика данных» (2025-2030 гг.):
Обеспечение функционирования Центра исследования безопасности системного ПО

Вопросы разработки СКЗИ. Новые/старые ГОСТы

- Разрешить использование ГОСТ 28147-89 после 1 июня 2024 г.
- ТЗ на разработку СКЗИ должны содержать поддержку новых ГОСТ, использование старых ГОСТ возможно для обеспечения совместимости работы с действующими ИС
- 8 Центр готов принимать изделия на КТИ без реализации в СКЗИ новых ГОСТ
- Возможно продление срока действия заключения и сертификата, ограниченных 1 июня 2024 г.


ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-4778 от "05" марта 2024 г.

Действителен до "28" февраля 2026 г.

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, классов КС1, КС2, КС3 для исполнений 1, 2, 3, соответственно, Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для классов КС1, КС2, КС3 для исполнений 1, 2, 3, соответственно, и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование файлов и данных, содержащихся в областях оперативной памяти, и IP-трафика, вычисление имитовставки для файлов и данных, содержащихся в областях оперативной памяти, и IP-трафика, вычисление значения хэш-функции для файлов и данных, содержащихся в областях оперативной памяти, создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) информации, не содержащей сведений, составляющих государственную тайну.

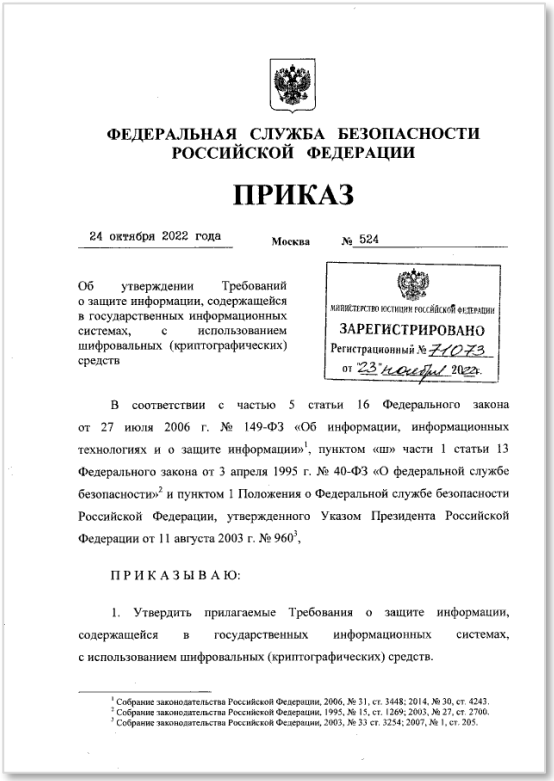
Сертификат выдан на основании результатов проведенных Обществом с ограниченной

сертификационных испытаний образцов продукции

Безопасность информации обеспечивается при использовании комплекса в соответствии с требованиями эксплуатационной документации согласно формуляру.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России О.В. Скрябин

ФСБ России.
Защита информации в ГИС



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

24 октября 2022 года Москва № 524

Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 71073
от 23 ноября 2022

В соответствии с частью 5 статьи 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[1], пунктом «ш» части 1 статьи 13 Федерального закона от 3 апреля 1995 г. № 40-ФЗ «О федеральной службе безопасности»[2] и пунктом 1 Положения о Федеральной службе безопасности Российской Федерации, утвержденного Указом Президента Российской Федерации от 11 августа 2003 г. № 960[3],

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемые Требования о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств.

[1] Собрание законодательства Российской Федерации, 2006, № 31, ст. 3448; 2014, № 30, ст. 4243.
[2] Собрание законодательства Российской Федерации, 1995, № 15, ст. 1269; 2003, № 27, ст. 2700.
[3] Собрание законодательства Российской Федерации, 2003, № 33 ст. 3254; 2007, № 1, ст. 205.

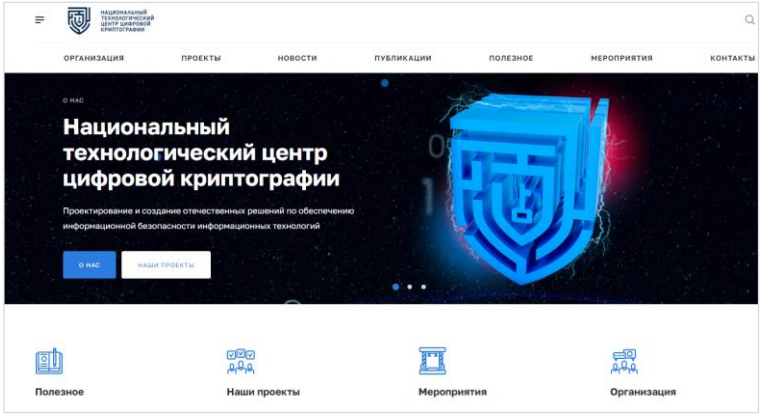
Приказ ФСБ России от 24 октября 2022 г. №524 «Об утверждении Требований о защите информации, содержащейся в ГИС, с использованием шифровальных (криптографических) средств»

- ✓ **распространяется на все ГИС не содержащие сведений, составляющих ГТ** (есть перечень исключений)
- ✓ необходимость использования СКЗИ для защиты информации, содержащейся в ГИС, подлежит обоснованию в модели угроз безопасности информации, которая согласуется с ФСБ России
- ✓ **вводятся Уровни значимости информации** в ГИС
- ✓ **допускается использование только сертифицированных в системе ФСБ России СКЗИ**
- ✓ **класс СКЗИ, используемых в ГИС, определяется для каждого сегмента ГИС**, либо для ГИС в целом, в случае если ГИС не содержит сегментов. В случае если ГИС состоит из двух и более сегментов ГИС, то уровень значимости информации и масштаб определяются для каждого сегмента отдельно

АНО «Национальный технологический центр цифровой криптографии»

Наиболее значимые результаты работы АНО «НТЦ ЦК» в 2023 г.

- Разработан экспериментальный образец Платформы цифрового доверия для подтверждения ПДн в процессах предоставления гражданам различных услуг
- Разработан и испытан прототип провайдера идентификации и аутентификации и программных библиотек протокола аутентификации OpenIDConnect с использованием российских криптографических средств и протоколов
- Развёрнута первая очередь системы «Мультисканер» для выявления вредоносного ПО в файлах, загружаемых в ГИС, включая вирусы-шифровальщики, с использованием антивирусных средств и технологий российских разработчиков
- Разработаны технические решения и методическое обеспечение по обезличиванию массивов ПДн для их безопасного использования при создании систем ИИ



На базе АНО НТЦ ЦК создан отраслевой центр ИБ цифровой экономики

Об ответственности компаний, работающих с ПДн

Ужесточились требования и повысилась ответственность компаний, работающих с ПДн

1 марта 2023 г. вступили в силу правки в ФЗ № 152 от 27 июня 2006 г., касающиеся уничтожения ПДн, их трансграничной передачи, порядка ведения учёта связанных с ними инцидентов и ряда иных моментов

4 декабря 2023 г. в Госдуму поступили для рассмотрения два законопроекта:

1. № 502113-8 «О внесении изменений в УК РФ»
   Устанавливается ответственность за незаконные использование и передачу, сбор и хранение компьютерной информации, содержащей ПДн

   Злоумышленников ждет ответственность в виде:
   - штрафов до 1 млн руб.
   - лишение свободы на срок до 6 лет
   - лишение права на занятие определенных должностей сроком до 3 лет

2. № 502104-8 «О внесении изменений в КоАП»
   Усиливается ответственность за нарушение порядка обработки ПДн

Правонарушение	Объем утечки ПДн (тыс. субъектов)	Штраф (рублей)
Первичное	1-10	3 000 000 (min)
	>100	15 000 000 (max)
Повторное	1-10	**15 000 000 (min)**
	>100	**500 000 000 (max)**

Цифровой рубль. Первые шаги

Новая форма национальной валюты

ИнфоТеКС представил подходы к реализации требований по обеспечению защиты инфраструктуры с использованием продуктов ViPNet для финансовых посредников – участников Платформы Цифрового рубля

https://infotecs.ru/press-center/events/zashchita-infrastruktury-tsifrovogo-rublya-dlya-kommercheskikh-bankov-pod-klyuch/

В 2023 году запущен пилотный проект операций с цифровым рублем с привлечением узкого круга клиентов 13 банков

В комплекс регламентирующих НПА вошли:

- Федеральный закон № 339-ФЗ от 24.07.2023
- Федеральный закон № 340-ФЗ от 24.07.2023
- Положение ЦБ РФ от 03.08.2023 № 820-П «О Платформе цифрового рубля»
- Положение ЦБ РФ от 07.12.2023 № 833-П «О требованиях к обеспечению защиты информации для участников платформы цифрового рубля»

Определяют:

- правовой статус
- порядок проведения операций
- и т.д.

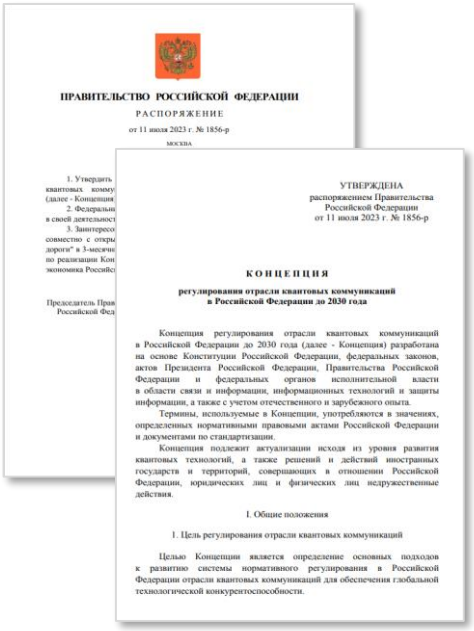
Концепция регулирования отрасли квантовых коммуникаций

Главное преимущество квантовых коммуникаций – защищенность передаваемой информации, гарантированная законами квантовой механики

Правительство РФ утвердило концепцию регулирования отрасли квантовых коммуникаций до 2030 г.

Основные задачи Концепции:

- **стимулирование развития рынка** квантовых коммуникаций
- **поддержка отечественных производителей**
- **достижение высокого уровня ИБ** граждан и гос. организаций



ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

РАСПОРЯЖЕНИЕ

от 11 июля 2023 г. № 1856-р

МОСКВА

УТВЕРЖДЕНА
распоряжением Правительства
Российской Федерации
от 11 июля 2023 г. № 1856-р

КОНЦЕПЦИЯ

регулирования отрасли квантовых коммуникаций
в Российской Федерации до 2030 года

Концепция регулирования отрасли квантовых коммуникаций в Российской Федерации до 2030 года (далее - Концепция) разработана на основе Конституции Российской Федерации, федеральных законов, актов Президента Российской Федерации, Правительства Российской Федерации и федеральных органов исполнительной власти в области связи и информации, информационных технологий и защиты информации, а также с учетом отечественного и зарубежного опыта.

Термины, используемые в Концепции, употребляются в значениях, определенных нормативными правовыми актами Российской Федерации и документами по стандартизации.

Концепция подлежит актуализации исходя из уровня развития квантовых технологий, а также решений и действий иностранных государств и территорий, совершающих в отношении Российской Федерации, юридических лиц и физических лиц недружественные действия.

I. Общие положения

1. Цель регулирования отрасли квантовых коммуникаций

Целью Концепции является определение основных подходов к развитию системы нормативного регулирования в Российской Федерации отрасли квантовых коммуникаций для обеспечения глобальной технологической конкурентоспособности.

В 2023 году Компания запустила собственный портал, посвященный квантовым технологиям в сфере ИБ – **Quantum Crypto**

Искусственный интеллект. Обеспечение защиты информации

Мероприятие национального проекта «Экономика данных» (2025-2030 гг.):
Обеспечение защиты информации при внедрении технологий ИИ. Повышение эффективности СЗИ и услуг по защите информации за счет применения технологий ИИ

Планируется создать Центр исследований в области обеспечения ИБ при использовании технологий ИИ

Задачи:

- Исследование угроз безопасности при применении технологий ИИ в системах защиты информации
- Разработка большой языковой модели для применения в СЗИ
- Разработка и поддержка в актуальном состоянии информационных ресурсов для информирования о новых угрозах и оценки вероятности атак на системы защиты информации, использующих технологии ИИ

Бонус на сегодня для организаций закупающих отечественные IT-решения

«…расходы, связанные с приобретением права на использование по договорам с правообладателем программ для ЭВМ и БД, включенных в единый реестр российского ПО, относящихся к сфере ИИ, **могут учитываться в размере фактических затрат с применением коэффициента 1,5**» (изменения в статьи 275 и 264 НК РФ)

infotecs

Спасибо за внимание!

Подписывайтесь на наши соцсети

https://vk.com/infotecs_news

https://t.me/infotecs_news