

Нормативно-техническое регулирование новых информационных технологий

Елистратов А.А.

A decorative graphic element consisting of several horizontal lines of varying lengths and colors (teal, light blue, white) extending from the right side of the slide towards the center.

Новые информационные технологии



ЦИКЛ ЗРЕЛОСТИ ТЕХНОЛОГИЙ



Новые информационные технологии

Hype Cycle for Emerging Technologies, 2020



Plateau will be reached:

○ less than 2 years

● 2 to 5 years

● 5 to 10 years

▲ more than 10 years

⊗ obsolete before plateau

As of July 2020

gartner.com/SmarterWithGartner

Source: Gartner
© 2020 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner and Hype Cycle are registered trademarks of Gartner, Inc. and its affiliates in the U.S.

Gartner

Новые информационные технологии

- Блокчейн
- «Интернет вещей»
- Квантовые технологии

Hype Cycle for Emerging Technologies, 2020



gartner.com/SmarterWithGartner

Source: Gartner
© 2020 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner and Hype Cycle are registered trademarks of Gartner, Inc. and its affiliates in the U.S.

Gartner

Новые информационные технологии

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

Hype Cycle for Emerging Technologies, 2020



gartner.com/SmarterWithGartner

Source: Gartner
© 2020 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner and Hype Cycle are registered trademarks of Gartner, Inc. and its affiliates in the U.S.

Gartner

Оценка соответствия требованиям по информационной безопасности в Российской Федерации

- В сфере своей компетенции вопросы информационной безопасности различных типов средств (криптографической) защиты информации (СЗИ и СКЗИ) и их использующих информационных систем отнесены к ведению:

ФСБ России, ФСТЭК России и Банка России.

Оценка соответствия требованиям по информационной безопасности в Российской Федерации

Банк России

- Положение Банка России от 9 июня 2012 г. № 382-П (Положение Банка России от 04.06.2020 N 719-П)

В данных документах указывается, в каких случаях следует использовать средства криптографической защиты информации, прошедшие оценку соответствия требованиям по информационной безопасности ФСБ России.

Оценка соответствия требованиям по информационной безопасности в Российской Федерации

ФСБ России

- Приказ ФСБ России от 9 февраля 2005 г. № 66 («Положение ПКЗ-2005»)»

В данном приказе определен порядок разработки, производства и эксплуатации средств криптографической защиты информации (СКЗИ).

Оценка соответствия требованиям по информационной безопасности в Российской Федерации

- если информация конфиденциального характера подлежит защите в соответствии с законодательством Российской Федерации;
- при организации криптографической защиты информации конфиденциального характера в государственных органах;
- при организации криптографической защиты информации конфиденциального характера в организациях, выполняющих государственные заказы;
- если обладатель информации принимает меры к охране ее конфиденциальности путем установления необходимости криптографической защиты данной информации.

Оценка соответствия требованиям по информационной безопасности в Российской Федерации

В Положении ПКЗ-2005 подробно описан порядок взаимодействия при разработке, производстве и эксплуатации СКЗИ между:

- заказчиком,
- разработчиком,
- специализированной организацией (выполняющей исследования по оценке соответствия СКЗИ требованиям по информационной безопасности),
- ФСБ России (оценивающей полноту и корректность проведенных исследований).

Данный порядок во многом схож с международными системами сертификации в различных областях.

Оценка соответствия требованиям по информационной безопасности в Российской Федерации

Непосредственно разработке и проведению тематических исследований предшествует согласование технического задания (ТЗ) на разработку СКЗИ в котором определяется:

- модель угроз и нарушителя;
- архитектура и предполагаемые условия эксплуатации;
- класс защиты СКЗИ (КС1, КС2, КС3, КВ, КА).

Блокчейн

- Статус:

В настоящее время технология успешно внедрена в:

Банковскую деятельность («Цифровые банковские гарантии», «Децентрализованная депозитарная система для учета закладных»)

и имеет применения в учетных системах грузоперевозок (пока только пилотные проекты).

Блокчейн

- На сегодняшний день для данной технологии в призме информационной безопасности нет необходимости вводить специальные требования.
- Блокчейн-решение формирует качественно новую сущность – достижение консенсуса при реализации протокола, доверие к которому формируется за счет использования криптографических атомарных запросов. Это фактически является определением криптографического протокола, а обеспечение защиты с использованием криптографических протоколов можно оценивать в рамках существующих требований.

Блокчейн

- Несмотря на то, что применение технологии блокчейн в первую очередь связывают с упрощением бизнес-процессов и устранением посредников, как показывает практика, уже на этапе построения модели угроз зачастую становится понятно, что разработчики не всегда в полной мере обладают информацией о фактически реализуемой в организации бизнес-логике.

Блокчейн

- При составлении модели угроз информации о реализуемой бизнес-логике должны быть рассмотрены сведения о функциях, выполняемых субъектами системы, их права, которые, в свою очередь и определяют возможный спектр угроз:
 - Может ли нарушитель являться администратором блокчейн-решения?
 - Может ли нарушитель являться пользователем блокчейн-решения?
 - Есть ли у нарушителя возможности (в том числе и потенциальные) влиять на работу модели блокчейн-решения в целом?
 - Является ли информация, обрабатываемая в блокчейн-решении, конфиденциальной?
 - Нужна ли юридическая значимость совершенных в блокчейн-решении действий?

Блокчейн

- Детально ознакомится с составом и содержанием требований к разработке СКЗИ можно из методических рекомендаций ТК26

Р 1323565.1.012-2017 «Информационная технология. Криптографическая защита информации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации»

«Интернет вещей»

- Статус

Широкое использование в коммерческой деятельности не связанной с обязательной оценкой соответствия требованиям по информационной безопасности.

Внедрено в значимые системы:

- контрольно-кассовой техники;
- тахографического контроля.

В проектах:

- промышленные счетчики и датчики.

«Интернет вещей»

- Все внедряемые системы «интернета вещей» на сегодняшний день имеют организацию типа «звезда» с центром в виде криптографического сервера.
- Оконечное оборудование объединяет одно специфичное свойство безопасности - некорректируемая регистрация данных.

«Интернет вещей»

- 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 корректировки;
 - возможность гарантированной аутентификации средства регистрации.

«Интернет вещей»

СКЗИ-НР

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

«Интернет вещей»

- СКЗИ-НР являются отдельным классом средств криптографической защиты информации, не содержащей сведений, составляющих государственную тайну, определяемым моделью нарушителя, рассматривающей в качестве нарушителя, в том числе, легального пользователя СКЗИ-НР, действующего строго в рамках определенных для него полномочий.
- 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

«Интернет вещей»

- Выписка из Требований к СКЗИ-НР доступна на сайте fsb.ru

<http://www.fsb.ru/fsb/science/single.htm%21id%3D10437338%40fsbResearchart.html>

Квантовые технологии

- Статус

В настоящее время системы квантовой криптографии активно разрабатываются как за рубежом, так и в России. Компания «Инфотекс» и Центр квантовых технологий МГУ представили первый в России телефон с квантовой защитой связи. (ViPNet QSS Phone).

Квантовые технологии

- В средствах массовой информации системы квантовой криптографии часто рекламируются в качестве абсолютно стойких систем шифрования, взлом которых невозможен даже при наличии у потенциального нарушителя неограниченных вычислительных мощностей и средств перехвата, ограниченных в своих возможностях только законами квантовой механики.
- При этом не афишируется, что достижение такого уровня стойкости возможно лишь при очень продуманном и тщательном синтезе квантовых криптографических протоколов и технической реализации систем квантовой криптографии.

Квантовые технологии

- Для обеспечения информационной безопасности Российских квантовых систем 20 июля 2017 года утверждены «Временные требования к квантовым криптографическим системам выработки и распределения ключей для средств криптографической защиты информации, не содержащей сведений, составляющих государственную тайну», ВТ ККС ВРК (СКЗИ).
- Данные требования достаточны для комплексной оценки безопасности систем квантовой криптографии.

Квантовые технологии

ВТ ККС ВРК 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.

Квантовые технологии

- Требования являются закрытыми, ознакомление с ними возможно только для организаций-лицензиатов ФСБ России, имеющих лицензию на соответствующий вид деятельности.
- Информация о созданных Требованиях доступна на сайте [fsb.ru](http://www.fsb.ru)

<http://www.fsb.ru/fsb/science/single.htm%21id%3D10438445%40fsbResearchart.html>.

Искусственный интеллект

- Статус

На текущем этапе - внедрение в различные коммерческие проекты.

Как и для любой технологии, которая начинает массово внедряться на практике, вопросы информационной безопасности пока что находятся на втором плане.

Искусственный интеллект

- Уже сейчас специалистами показана возможность реализации широкого спектра атак, специфичных для систем машинного обучения. Эта специфика связана с тем, что такие системы наряду с ответом на решаемый вопрос формируют и сам алгоритм решения.
- С технической точки зрения это разбивает процесс функционирования систем машинного обучения, как активно обсуждаемых в настоящее время нейросетевых, так и классических статистических, на две фазы: обучения и работы.

Искусственный интеллект

- **Атаки на процесс обучения** в большинстве своем направлены на изменение последующей логики функционирования системы за счет подачи на вход специальным образом сформированных данных (т. н. отравленных). Это может привести к внедрению в систему закладок, когда алгоритм, например, будет распознавать лицо нарушителя, которое находилось среди отравленных данных, как легитимного пользователя, либо такое внедрение может привести к общему ухудшению качества работы (увеличения ошибок распознавания).

Искусственный интеллект

- **Атаки на этапе работы** известны более широко, в первую очередь, благодаря частому упоминанию в СМИ:
- «Дипфейки» - сформированные с использованием нейронных сетей синтетические изображения, которые могут распознаваться системами ИИ, а зачастую и людьми, как настоящие. В ряде случаев, например, имеется возможность построения входных изображений биометрических систем идентификации, которые человеком могут восприниматься одним образом, а системой искусственного интеллекта — другим. Такие синтетические образы несут серьезную опасность для систем удаленной биометрической идентификации.

Искусственный интеллект

- **Атаки на этапе работы**
 - нарушение конфиденциальность данных, использованных при обучении нейронных сетей, - атаки, позволяющие извлекать данные об обучающей выборке из обученной нейронной сети.

Искусственный интеллект

- Методы защиты систем искусственного интеллекта:
 - статистическое обезличивание, заключающееся в зашумлении защищаемых данных, подлежащих статистической обработке.
 - гомоморфное шифрование, которое хотя в общем случае пока еще слабо применимо к реальным задачам, в случае задачи защиты статистических и нейросетевых методов, по оценкам специалистов, позволяет достигать приемлемых эксплуатационных характеристик.
 - протоколы распределенных безопасных вычислений, которые позволяют группе операторов персональных данных производить совместную аналитику без раскрытия самих данных.

Искусственный интеллект

- В настоящее время требований по информационной безопасности систем искусственного интеллекта в Российской Федерации нет.
- Теоретические и практические вопросы построения защищенных систем искусственного интеллекта включены в федеральный проект «Искусственный интеллект» национальной программы «Цифровая экономика Российской Федерации».

Выводы

- Блокчейн – не требует дополнительного регулирования
- «Интернет вещей» – созданы требования
- Квантовые технологии – созданы требования
- Искусственный интеллект – требований нет

- Спасибо за внимание