Есть ли жизнь после ГОСТ 28147-89?

Д.В. Матюхин

ФСБ России

РусКрипто'2018

Почему появился этот доклад?

Почему появился этот доклад?

- 1 мая 2018 года вводятся в действие Р 1323565.1.012-2017 Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации

Почему появился этот доклад?

- 1 мая 2018 года вводятся в действие Р 1323565.1.012-2017 Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации
- предписывают использовать криптографические механизмы, определяемые национальными стандартами Российской Федерации, рекомендациями по стандартизации Росстандарта или имеющие положительное заключение ФСБ России по результатам их экспертных криптографических исследований

Почему появился этот доклад?

- 1 мая 2018 года вводятся в действие Р 1323565.1.012-2017 Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации
- предписывают использовать криптографические механизмы, определяемые национальными стандартами Российской Федерации, рекомендациями по стандартизации Росстандарта или имеющие положительное заключение ФСБ России по результатам их экспертных криптографических исследований
- ГОСТ 28147-89 определяет базовый блочный шифр *и* его режимы

Почему появился этот доклад?

- 1 мая 2018 года вводятся в действие Р 1323565.1.012-2017 Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации
- предписывают использовать криптографические механизмы, определяемые национальными стандартами Российской Федерации, рекомендациями по стандартизации Росстандарта или имеющие положительное заключение ФСБ России по результатам их экспертных криптографических исследований
- ГОСТ 28147-89 определяет базовый блочный шифр *и* его режимы
- ГОСТ Р 34.12-2015 определяет базовые блочные шифры «Кузнечик» и «Магма» = ГОСТ 28147-89 *в режиме простой замены с фиксированным блоком подстановки*

Почему появился этот доклад?

- 1 мая 2018 года вводятся в действие Р 1323565.1.012-2017 Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации
- предписывают использовать криптографические механизмы, определяемые национальными стандартами Российской Федерации, рекомендациями по стандартизации Росстандарта или имеющие положительное заключение ФСБ России по результатам их экспертных криптографических исследований
- ГОСТ 28147-89 определяет базовый блочный шифр *и* его режимы
- ГОСТ Р 34.12-2015 определяет базовые блочные шифры «Кузнечик» и «Магма» = ГОСТ 28147-89 *в режиме простой замены с фиксированным блоком подстановки*
- ГОСТ Р 34.13-2015 определяет режимы работы блочных шифров, бóльшая часть которых *отлична* от режимов, определяемых ГОСТ 28147-89

Почему появился этот доклад?

- ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015 *не отменяют* ГОСТ 28147-89, который имеет статус межгосударственного стандарта

Почему появился этот доклад?

- ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015 *не отменяют* ГОСТ 28147-89, который имеет статус межгосударственного стандарта
- В настоящее время идёт обновление межгосударственных стандартов в области криптографической защиты информации на базе ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015. Планируемый срок завершения – ноябрь 2018

Почему появился этот доклад?

- ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015 *не отменяют* ГОСТ 28147-89, который имеет статус межгосударственного стандарта
- В настоящее время идёт обновление межгосударственных стандартов в области криптографической защиты информации на базе ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015. Планируемый срок завершения – ноябрь 2018
- Первые редакции проектов межгосударственных стандартов на базе ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015 предусматривают *отмену* ГОСТ 28147-89

Почему появился этот доклад?

- ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015 *не отменяют* ГОСТ 28147-89, который имеет статус межгосударственного стандарта
- В настоящее время идёт обновление межгосударственных стандартов в области криптографической защиты информации на базе ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015. Планируемый срок завершения – ноябрь 2018
- Первые редакции проектов межгосударственных стандартов на базе ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015 предусматривают *отмену* ГОСТ 28147-89
- В настоящем докладе будут изложены *предполагаемые* действия регулятора в отношении использования криптографических механизмов, определяемых ГОСТ 28147-89, в случае принятия указанных межгосударственных стандартов

Что может произойти в случае отмены ГОСТ 28147-89?

Что может произойти в случае отмены ГОСТ 28147-89?

- в отношении ГОСТ 28147-89 *в режиме простой замены с рекомендованными значениями блока подстановки* будет утверждено положительное заключение ФСБ России по результатам экспертных криптографических исследований

Что может произойти в случае отмены ГОСТ 28147-89?

- в отношении ГОСТ 28147-89 *в режиме простой замены с рекомендованными значениями блока подстановки* будет утверждено положительное заключение ФСБ России по результатам экспертных криптографических исследований
- это сделает возможным использование *указанного* криптографического механизма в шифровальных (криптографических) средствах защиты информации, не содержащей сведений, составляющих государственную тайну

Что может произойти в случае отмены ГОСТ 28147-89?

- в отношении ГОСТ 28147-89 *в режиме простой замены с рекомендованными значениями блока подстановки* будет утверждено положительное заключение ФСБ России по результатам экспертных криптографических исследований
- это сделает возможным использование *указанного* криптографического механизма в шифровальных (криптографических) средствах защиты информации, не содержащей сведений, составляющих государственную тайну
- заключение *не будет* распространяться на режимы работы, определяемые ГОСТ 28147-89, но не определяемые ГОСТ Р 34.13-2015, и значения блока подстановки, не являющиеся рекомендованными

Что может произойти в случае отмены ГОСТ 28147-89?

- опубликован список рекомендованных значений блока подстановки, возможно, включающий некоторые из уже используемых значений

Что может произойти в случае отмены ГОСТ 28147-89?

- опубликован список рекомендованных значений блока подстановки, возможно, включающий некоторые из уже используемых значений
- при необходимости ФСБ России будут вырабатываться дополнительные рекомендованные значения блока подстановки

Что может произойти в случае отмены ГОСТ 28147-89?

- опубликован список рекомендованных значений блока подстановки, возможно, включающий некоторые из уже используемых значений
- при необходимости ФСБ России будут вырабатываться дополнительные рекомендованные значения блока подстановки
- объявлен 5-летний переходный период, по истечении которого использование криптографических механизмов, удовлетворяющих ГОСТ 28147-89, на которые не распространяется действие заключения, в случаях, подлежащих регулированию со стороны ФСБ России, не допускается

Вместо эпилога

Вместо эпилога

- ГОСТ Р 34.13-2015 определяет существенно больше режимов работы блочных шифров по сравнению с ГОСТ 28147-89, но ограничивается только функциями шифрования и имитозащиты

Вместо эпилога

- ГОСТ Р 34.13-2015 определяет существенно больше режимов работы блочных шифров по сравнению с ГОСТ 28147-89, но ограничивается только функциями шифрования и имитозащиты
- завершена разработка проекта методических рекомендаций ТК 26, определяющих алгоритм выработки псевдослучайных последовательностей с использованием блочного шифра

Вместо эпилога

- ГОСТ Р 34.13-2015 определяет существенно больше режимов работы блочных шифров по сравнению с ГОСТ 28147-89, но ограничивается только функциями шифрования и имитозащиты
- завершена разработка проекта методических рекомендаций ТК 26, определяющих алгоритм выработки псевдослучайных последовательностей с использованием блочного шифра
- завершена экспертиза проектов режима аутентифицированного шифрования (см. программу конференции)

Вместо эпилога

- ГОСТ Р 34.13-2015 определяет существенно больше режимов работы блочных шифров по сравнению с ГОСТ 28147-89, но ограничивается только функциями шифрования и имитозащиты
- завершена разработка проекта методических рекомендаций ТК 26, определяющих алгоритм выработки псевдослучайных последовательностей с использованием блочного шифра
- завершена экспертиза проектов режима аутентифицированного шифрования (см. программу конференции)
- автор доклада выражает благодарность Г.Б. Маршалко как автору названия доклада