ЕВРАЗИЙСКАЯ ЭКОНОМИЧЕСКАЯ КОМИССИЯ
КОЛЛЕГИЯ

Р Е К О М Е Н Д А Ц И Я

«12» марта 2019 г. **№ 9** г. Москва

О перечне стандартов и рекомендаций в области информационной безопасности, применяемых в рамках реализации цифровой повестки Евразийского экономического союза

Коллегия Евразийской экономической комиссии в целях унификации применяемых в рамках реализации цифровой повестки Евразийского экономического союза подходов к обеспечению информационной безопасности

рекомендует государствам – членам Евразийского экономического союза с даты опубликования настоящей Рекомендации на официальном сайте Евразийского экономического союза при проведении работ в рамках реализации цифровой повестки Евразийского экономического союза применять в соответствии с законодательством государств – членов Евразийского экономического союза стандарты и рекомендации в области информационной безопасности по перечню согласно приложению.

Председатель Коллегии
Евразийской экономической комиссии В. Саркисян

ПРИЛОЖЕНИЕ

Рекомендации Коллегии
Евразийской экономической комиссии
от 12 марта 2019 г. № 9

ПЕРЕЧЕНЬ
стандартов и рекомендаций в области информационной безопасности, применяемых в рамках реализации цифровой повестки Евразийского экономического союза

I. Разработка средств защиты информации и разработка приложений

1. ISO/IEC/IEEE 12207:2017 «Системная и программная инженерия. Процессы жизненного цикла программных средств» (Systems and software engineering – Software life cycle processes).

2. ГОСТ ИСО/МЭК 12207-2002 «Информационная технология. Процессы жизненного цикла программных средств».

3. СТ РК ISO/IEC 12207-2015 «Системная и программная инженерия. Процессы жизненного цикла программных средств».

4. ISO/IEC 27031:2011 «Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса» (Information technology – Security techniques – Guidelines for information and communications technology readiness for business continuity).

5. СТ РК ISO/IEC 27031-2013 «Информационные технологии. Методы обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий для обеспечения непрерывности бизнеса».

6. ISO/IEC 15408-1:2009 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ. Часть 1. Введение и общая модель» (Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model).

7. СТ РК ISO/IEC 15408-1-2017 «Информационные технологии. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель».

8. СТБ 34.101.1-2014 (15408-1:2009) «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель».

9. ISO/IEC 15408-2:2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ. Часть 2. Функциональные требования безопасности» (Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional components).

10. СТ РК ISO/IEC 15408-2-2017 «Информационные технологии. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности».

11. СТБ 34.101.2-2014 (15408-2:2009) «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности».

12. ISO/IEC 15408-3:2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ. Часть 3. Требования к обеспечению защиты» (Information

technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance components).

13. СТ РК ISO/IEC 15408-3-2017 «Информационные технологии. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования обеспечению защиты».

14. СТБ 34.101.3-2014 (15408-3:2009) «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3. Гарантийные требования безопасности».

II. Создание и сопровождение систем управления информационной безопасностью

15. СТБ ISO/IEC 27000-2012 «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Основные положения и словарь».

16. ISO/IEC 27001:2013 «Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (Information technology - Security techniques - Information security management systems - Requirements).

17. СТ РК ISO/IEC 27001-2015 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасностью. Требования».

18. СТБ ISO/IEC 27001-2016 «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

19. ISO/IEC 27002:2013 «Информационные технологии. Методы обеспечения безопасности. Свод правил по управлению защитой

информации» (Information technology - Security techniques - Code of practice for information security controls).

20. СТ РК ISO/IEC 27002-2015 «Информационная технология. Методы и средства обеспечения безопасности. Свод правил по средствам управления защитой информации».

21. СТБ ISO/IEC 27002-2012 «Информационные технологии. Методы обеспечения безопасности. Кодекс практики для менеджмента информационной безопасности».

22. ISO/IEC 27003:2017 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство» (Information technology – Security techniques – Information security management systems –Guidance).

23. СТ РК ISO/IEC 27003-2012 «Информационные технологии. Методы обеспечения безопасности. Руководство по внедрению системы менеджмента информационной безопасности».

24. СТБ ISO/IEC 27003-2014 «Информационные технологии. Методы обеспечения безопасности. Руководство по внедрению системы менеджмента информационной безопасности».

25. ISO/IEC 27004:2016 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, измерения, анализ и оценка» (Information technology – Security techniques – Information security management – Monitoring, measurement, analysis).

26. СТ РК ISO/IEC 27004-2012 «Информационные технологии. Методы обеспечения безопасности. Менеджмент информационной безопасности. Измерение».

27. СТБ ISO/IEC 27004-2014 «Информационные технологии. Методы обеспечения безопасности. Менеджмент информационной безопасности. Измерения».

28. ISO/IEC 27005:2018 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» (Information technology – Security techniques – Information security risk management).

29. СТ РК ISO/IEC 27005-2013 «Информационные технологии. Методы обеспечения безопасности. Менеджмент риска информационной безопасности».

30. СТБ ISO/IEC 27005-2012 «Информационные технологии. Методы обеспечения безопасности. Менеджмент рисков информационной безопасности».

31. СТБ ISO/IEC 27006-2018 «Информационные технологии. Методы обеспечения безопасности. Требования к органам, проводящим аудит и сертификацию систем менеджмента информационной безопасности».

32. СТБ ISO/IEC 27011-2017 «Информационные технологии. Методы обеспечения безопасности. Руководство по менеджменту информационной безопасности для организаций телекоммуникационной отрасли на основе ISO/IEC 27002».

33. СТБ ISO/IEC 27035-2017 «Информационные технологии. Методы обеспечения безопасности. Менеджмент инцидентов в области информационной безопасности».

34. СТБ 34.101.70-2016 «Информационные технологии. Методы и средства безопасности. Методика оценки рисков информационной безопасности в информационных системах».

III. Обеспечение сетевой безопасности и обеспечение защиты веб-сервисов

35. ISO/IEC 27033-1:2015 «Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 1. Обзор и концепции» (Information technology - Security techniques - Network security - Part 1: Overview and concepts).

36. СТ РК ISO/IEC 27033-1-2017 «Информационные технологии. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 1. Обзор и концепции».

37. ISO/IEC 27033-2:2012 «Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 2. Руководящие принципы по разработке и внедрению средств обеспечения безопасности сетей» (Information technology - Security techniques - Network security - Part 2: Guidelines for the design and implementation of network security).

38. СТ РК ISO/IEC 27033-2-2017 «Информационные технологии. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 2. Руководящие указания по проектированию и внедрению защиты сети».

39. ISO/IEC 27033-3:2010 «Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления» (Information technology - Security techniques - Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues).

40. ISO/IEC 27033-4:2018 «Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 4. Коммуникации для обеспечения безопасности между сетями с

применением шлюзов безопасности» (Information technology - Security techniques - Network security - Part 4: Securing communications between networks using security gateways).

41. СТ РК ISO/IEC 27033-4-2017 «Информационные технологии. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 4. Коммуникации для обеспечения безопасности между сетями с применением шлюзов безопасности».

42. ISO/IEC 27033-5:2013 «Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 5. Безопасное межсетевое взаимодействие с использованием виртуальных частных сетей (VPNs)» (Information technology - Security techniques - Network security - Part 5: Securing communications across networks using Virtual Private Networks (VPNs)).

43. СТ РК ISO/IEC 27033-5-2017 «Информационные технологии. Методы обеспечения безопасности. Сетевая безопасность. Часть 5. Коммуникации для обеспечения безопасности между сетями с применением виртуальных частных сетей (VPN)».

44. ISO/IEC 27033-6:2018 «Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 6. Защищенный доступ к беспроводной IP-сети» (Information technology - Security techniques - Network security - Part 6: Securing wireless IP network access).

45. СТ РК ISO IEC 27033-6-2017 «Информационные технологии. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 6. Защищенный доступ к беспроводной IP-сети».

46. ISO/IEC 27039:2015 «Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность. Выбор, внедрение и сопровождение систем обнаружения и предотвращения

вторжений» (Information technology - Security techniques - Selection, deployment and operations of intrusion detection and prevention systems (IDPS)).

47. Спецификация безопасности веб-сервисов «Безопасность структурированных сообщений» (Web Services Security: SOAP Message Security 1.1 (WS-Security 2004)).

48. Руководящие принципы по обеспечению доступности веб-контента (Web Content Accessibility Guidelines (WCAG) 2.1).

49. СТ РК ИСО/МЭК 18028-4-2007 «Технологии информационные. Методы обеспечения защиты. Защита сети информационных технологий. Часть 4. Защита удалённого доступа».

50. СТБ 34.101.8-2006 «Информационные технологии. Методы и средства безопасности. Программные и программно-аппаратные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Общие требования».

51. СТБ 34.101.14-2017 «Информационные технологии. Методы и средства безопасности. Программные средства маршрутизатора. Общие требования».

52. СТБ 34.101.37-2017 «Информационные технологии и безопасность. Методы и средства безопасности. Системы управления сайта. Общие требования».

53. СТБ 34.101.73-2017 «Информационные технологии. Методы и средства безопасности. Межсетевые экраны. Общие требования».

54. СТБ 34.101.74-2017 «Информационные технологии. Системы сбора и обработки данных событий информационной безопасности. Общие требования».

55. СТБ 34.101.75-2017 «Информационные технологии. Системы обнаружения и предотвращения вторжений. Общие требования».

56. СТБ 34.101.76-2017 «Информационные технологии. Методы и средства безопасности. Системы обнаружения и предотвращения утечек информации из информационных систем. Общие требования».

IV. Обеспечение защиты информации с использованием средств криптографической защиты

57. Спецификация безопасности на транспортном уровне TLS 1.2: RFC 5246 (A Transport Layer Security (TLS) Protocol Version 1.2).

58. Спецификация безопасности на транспортном уровне TLS 1.3: RFC 8446 (The Transport Layer Security (TLS) Protocol Version 1.3).

59. Набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IPSec: RFC 2401, RFC 2402, RFC 2403, RFC 2404, RFC 2405, RFC 2406, RFC 2407, RFC 2408, RFC 2409, RFC 2410, RFC 2411, RFC 2412.

60. ГОСТ 34.12-2018 «Информационная технология. Криптографическая защита информации. Блочные шифры».

61. ГОСТ 34.13-2018 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров».

62. Рекомендации по стандартизации Р 1323565.1.020-2018 «Информационная технология. Криптографическая защита информации. Использование криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)».

63. Рекомендации по стандартизации Р 1323565.1.022-2018 «Информационная технология. Криптографическая защита информации. Функции выработки производного ключа»

64. Рекомендации по стандартизации Р 1323565.1.017-2018 «Информационная технология. Криптографическая защита

информации. Криптографические алгоритмы, сопутствующие применению алгоритмов блочного шифрования».

65. Рекомендации по стандартизации Р 1323565.1.005-2017 «Информационная технология. Криптографическая защита информации. Допустимые объемы материала для обработки на одном ключе при использовании некоторых вариантов режимов работы блочных шифров в соответствии с ГОСТ Р 34.13-2015».

66. Рекомендации по стандартизации Р 1323565.1.004-2017 «Информационная технология. Криптографическая защита информации. Схемы выработки общего ключа с аутентификацией на основе открытого ключа».

67. Рекомендации по стандартизации Р 50.1.114–2016 «Информационная технология. Криптографическая защита информации. Параметры эллиптических кривых для криптографических алгоритмов и протоколов».

68. Рекомендации по стандартизации Р 50.1.113–2016 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования».

69. СТБ 34.101.47-2017 «Информационные технологии и безопасность. Криптографические алгоритмы генерации псевдослучайных чисел».

70. СТБ 34.101.60-2014 «Информационные технологии и безопасность. Алгоритмы разделения секрета».

71. СТБ 34.101.66-2014 «Информационные технологии и безопасность. Протоколы формирования общего ключа на основе эллиптических кривых».

V. Обеспечение возможности использования электронной цифровой подписи (электронной подписи) и обеспечение функционирования сервисов доверенной третьей стороны

72. Спецификация управления ключами XML-подписей (XML Key Management Specification (XKMS 2.0) Version 2.0 W3C Recommendation 28 June 2005).

73. ITU-T X.842 «Информационные технологии. Методы защиты. Руководящие указания по применению и управлению службами доверенной третьей стороны» (Information technology - Security techniques - Guidelines for the use and management of trusted third party services).

74. ITU-T X.509 «Информационные технологии. Взаимосвязь открытых систем. Справочник: Структуры сертификатов открытых ключей и атрибутов» (Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks).

75. Синтаксис и обработка электронной подписи в XML (XML Signature Syntax and Processing (Second Edition) (XML-DSig)).

76. Расширение электронной подписи в XML (XML Advanced Electronic Signatures (XAdES)).

77. Расширение электронной подписи в PDF (PDF Advanced Electronic Signatures (PadES)).

78. CMS Hасширение электронной подписи (CMS Advanced Electronic Signatures (CadES)).

79. RFC 5280 «Профили сертификатов и списков отозванных сертификатов в инфраструктуре открытых ключей Internet X.509» (Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile).

80. RFC 6818 «Дополнение к профилям сертификатов и списков отозванных сертификатов в инфраструктуре открытых ключей Internet X.509» (Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile).

81. RFC 4210 «Протокол управления сертификатами в инфраструктуре открытых ключей Internet X.509 » (Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)).

82. PKCS#11 «Интерфейс взаимодействия с криптографическими токенами» (PKCS#11 Cryptographic Token Interface).

83. ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».

84. СТБ 34.101.45-2013 «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых».

85. ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования».

86. СТБ 34.101.31-2011 «Информационные технологии и безопасность. Криптографические алгоритмы шифрования и контроля целостности».

87. ГОСТ 34.10-2018 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».

88. ГОСТ 34.11-2018 «Информационная технология. Криптографическая защита информации. Функция хэширования».

89. Рекомендации по стандартизации Р 1323565.1.023-2018 «Информационная технология. Криптографическая защита информации. Использование алгоритмов ГОСТ Р 34.10-2012, ГОСТ Р

34.11-2012 в сертификате, списке аннулированных сертификатов (CRL) и запросе на сертификат PKCS #10 инфраструктуры открытых ключей X.509».

90. СТБ 34.101.17-2012 «Информационные технологии и безопасность. Синтаксис запроса на получение сертификата».

91. СТБ 34.101.18-2009 «Информационные технологии. Синтаксис обмена персональной информацией».

92. СТБ 34.101.19-2012 «Информационные технологии и безопасность. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей».

93. СТБ 34.101.23-2012 «Информационные технологии и безопасность. Синтаксис криптографических сообщений».

94. СТБ 34.101.26-2012 «Информационные технологии и безопасность. Онлайновый протокол проверки статуса сертификата (OCSP)».

95. СТБ 34.101.48-2012 «Информационные технологии и безопасность. Требования к политике применения сертификатов удостоверяющих центров».

96. СТБ 34.101.65-2014 «Информационные технологии и безопасность. Протокол защиты транспортного уровня (TLS)».

97. СТБ 34.101.67-2014 «Информационные технологии и безопасность. Инфраструктура атрибутных сертификатов».

98. СТБ 34.101.77-2016 «Информационные технологии и безопасность. Алгоритмы хэширования».

99. СТБ 34.101.78-2018 «Информационные технологии и безопасность. Профиль инфраструктуры открытых ключей».

100. СТБ 34.101.79-2018 «Информационные технологии и безопасность. Криптографические токены».

101. СТБ 34.101.80-2018 «Информационные технологии и безопасность. Расширенные электронные цифровые подписи».

102. СТБ 34.101.81-2018 «Информационные технологии и безопасность. Протоколы службы заверения данных».

103. СТБ 34.101.82-2018 «Информационные технологии и безопасность. Протокол простановки штампа времени».

VI. Обеспечение доверия к цифровым сервисам

104. ISO 19011:2018 «Руководство по аудиту систем менеджмента» (Guidelines for auditing management systems).

105. СТБ 34.101.27-2011 «Информационные технологии и безопасность. Требования безопасности к программным средствам криптографической защиты информации».

VII. Обеспечение функций по идентификации субъектов электронного взаимодействия, в том числе сервисов информационно-коммуникационных технологий, и проверке правомочий

106. ISO/IEC 9594-8:2017 «Информационная технология. Взаимосвязь открытых систем. Справочник. Часть 8. Структура сертификата на открытый ключ и атрибуты» (Information technology – Open Systems Interconnection – The Directory – Part 8: Public-key and attribute certificate frameworks).

107. RFC 5755 «Профиль атрибутивного сертификата для авторизации» (An Internet Attribute Certificate Profile for Authorization).