ГОСУДАРСТВЕННЫЙ СТАНДАРТ УЗБЕКИСТАНА

Информационная технология
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ
Термины и определения

Издание официальное

Узбекское агентство стандартизации, метрологии и сертификации

Ташкент

Предисловие

1 РАЗРАБОТАН Государственным унитарным предприятием Центр научно-технических и маркетинговых исследований «UNICON.UZ» - (ГУП «UNICON.UZ»)

2 ВНЕСЕН Техническим комитетом по стандартизации в сфере связи, информатизации и текоммуникационных технологий № 7

3 УТВЕРЖДЕН постановлением Узбекского агентства стандартизации, метрологии и сертификации (агентство «Узстандарт») от 15.07.2013 № 05-475

4 ВЗАМЕН O‘z DSt 1109:2006

5 В настоящем стандарте реализованы нормы законов Республики Узбекистан «Об электронной цифровой подписи» и «Об электронном документообороте»

Информация о введении в действие (прекращении действия) настоящего стандарта и изменений к нему на территории Узбекистана публикуется в указателе, издаваемом агентством «Узстандарт». В случае пересмотра или отмены настоящего стандарта соответствующая информация будет опубликована в информационном указателе, издаваемом агентством «Узстандарт»

Исключительное право официального опубликования настоящего стандарта на территории Узбекистана принадлежит агентству «Узстандарт»

II O‘ZBEKISTON AGENTLIGI STANDARTLASHTIRISH, DAVLAT NAZORATINI MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARINI JORIY ETISH BOSHQARMASI

Содержание

1 Область применения 1
2 Термины и определения 2
3 Алфавитный указатель терминов на русском языке 48
4 Алфавитный указатель терминов на узбекском языке 55
5 Алфавитный указатель терминов на английском языке 62

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

ГОСУДАРСТВЕННЫЙ СТАНДАРТ УЗБЕКИСТАНА

Ахборот технологияси
АХБОРОТНИНГ КРИПТОГРАФИК МУҲОФАЗАСИ
Атамалар ва таърифлар

Информационная технология
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ
Термины и определения

Information technologies. Cryptographic data security.
Terms and definitions

Дата введения 19.07.2013
ўтказилган

1 Область применения

Настоящий стандарт устанавливает основные термины и их определения в области криптографической защиты информации.

Установленные термины обязательны для применения во всех видах документации.

В данном стандарте приведены эквиваленты стандартизованных терминов на узбекском (uz) и английском (en) языках.

Для удобства пользования стандартом приведены в алфавитном порядке указатели терминов на русском, узбекском и английском языках с указанием соответствующих номеров терминологических статей.

O'ZSTANDART AGENTLIGI
4186 son bilan
«15» 08 2013 yilda
Davlat ro'yxatiga olindi

Издание официальное

2 Термины и определения

Термин	Определение
2.1 Общие понятия	
2.1.1 авторизация: uz – авторизация қилиш en – authorization	1 Определение полномочий и уровня доступа пользователя, подключившегося к системе, после успешного прохождения этапа аутентификации. 2 Предоставление доступа к различным системным ресурсам или отказ в доступе.
2.1.2 администрация безопасности: uz – хавфсизлик маъмурияти en - security administration	1 Полномочный представитель (лицо или группа лиц), ответственный за обеспечение безопасности системы, за реализацию и непрерывность соблюдения установленных административных мер защиты и осуществляющий постоянную организационную поддержку функционирования применяемых физических и технических средств защиты. 2 Должностное лицо, которое устанавливает политику безопасности, а также идентифицирует объекты и участников, к которым применяется политика.
2.1.3 алгоритм: uz – алгоритм en – algorithm	Упорядоченный конечный набор четко определенных правил для решения задач за конечное количество шагов.
2.1.4 алгоритм ограниченного использования: uz – фойдаланилиши чекланган алгоритм en – limited use algorithm	Криптосистема, стойкость которой основана на секретности алгоритма.
2.1.5 алгебраическая степень нелинейности булевой функции: uz – буль функция-сининг алгебраик чизиқсизлик даражаси en –algebraic degree of nonlinearity of Boolean function	Количество сомножителей в крайнем правом элементе алгебраической нормальной формы булевой функции.

O'z STANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT NAZORATINI MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARINI JORIY ETISH BOSHQARMASI

Термин		Определение
2.1.6	**аутентификация:** uz – аутентификация қилиш (ҳақиқийликни тасдиқлаш) en – authentication	Процедура установления подлинности пользователя (абонента сети, отправителя сообщения), программы, устройства или данных (информации, получаемого сообщения, ключа).
2.1.7	**аутентификация пользователя:** uz – фойдаланувчини аутентификация қилиш en – user authentication	Процесс, разработанный для проверки истинности заявки пользователя относительно своей идентичности.
2.1.8	**аутентификация сообщения:** uz – хабарни аутентификация қилиш en – message authentication	Проверка того, что сообщение было послано неповрежденным, неизмененным и от подразумеваемого отправителя предназначенному получателю.
2.1.9	**аутентичность:** uz – ҳақиқийлик en – authenticity	1 Свойство данных быть подлинными или свойство систем быть способными обеспечить подлинность данных. 2 Избежание недостатка полноты или точности при санкционированных изменениях информации.
2.1.10	**аутентичный канал:** uz – ҳақиқий канал en – the authentic channel	Открытый канал, гарантирующий подлинность источника информации (открытого ключа отправителя).
2.1.11	**байт:** uz – байт en – byte	Единица измерения информации равная 8 bit.
2.1.12	**бит:** uz – бит en – bit	Двоичный разряд машинного кода; элементарная единица информации, принимающая значение 0 или 1 в двоичной системе счисления.
2.1.13	**биометрия:** uz – биометрия en – biometrics	1 Наука об использовании для идентификации личности биологических свойств, например, отпечатков пальцев или голоса. 2 Методы автоматической идентификации личности человека, основанные на физиологических характеристиках.

O ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI

Термин	Определение
2.1.14 **биометрическая аутентификация:** uz – биометрик аутентификация қилиш en – biometric authentication	Аутентификация пользователя по его биометрическим признакам, например, отпечаткам пальцев, структуре сетчатки глаза, особенностям голоса и т.д.
2.1.15 **биометрическая идентификация:** uz – биометрик идентификация қилиш en – biometric identification	Процесс создания модели, описывающей с заданными значениями ошибок первого и второго рода совокупность биометрических образов конкретной личности в рамках заданного способа наблюдения биометриических образов и в рамках заданного способа измерения контролируемых биометрических параметров.
2.1.16 **биометрическая система:** uz – биометрик тизим en – biometric(al) system	1 Техническая система, построенная на измерении биометрических параметров личности, способная после обучения узнавать личность. 2 Система идентификации или верификации личности человека на основе его биометрических характеристик (например, отпечатков пальцев, геометрии руки, параметров лица и радужной оболочки глаз).
2.1.17 **блок:** uz – блок en – block	1 Совокупность данных, которые вводятся или выводятся одновременно. 2 Последовательность битов, имеющая фиксированную длину.
2.1.18 **вектор инициализации:** uz – инициализация вектори en – initialization vector	1 Вектор, используемый для определения отправной точки криптографического процесса в пределах криптографического алгоритма. 2 Случайное число, которое регулярно обновляется, передается по каналу управления и используется для инициализации алгоритма шифрования.
2.1.19 **владелец информации:** uz – ахборот эгаси en – information owner	Субъект информационных отношений, обладающий правом владения, распоряжения и пользования информационным ресурсом по договору с собственником информации.

© STANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

	Термин	Определение
2.1.20	**временный ключ:** uz – вақтинчалик калит en – temporary key	Сеансовый ключ, используемый в симметричных системах шифрования. Примечание – Для шифрования каждого сеанса применяется новый ключ.
2.1.21	**гамма шифра:** uz – шифр гаммаси en – gamma of the cipher	1 Случайная или псевдослучайная двоичная последовательность, вырабатываемая по заданному алгоритму для зашифрования открытых данных и расшифрования зашифрованных данных. 2 Псевдослучайная последовательность, вырабатываемая по определенному алгоритму для шифрования информации.
2.1.22	**гаммирование:** uz – гаммалаш en – gamming	Процесс наложения по определенному закону гаммы шифра на открытые данные для их зашифрования.
2.1.23	**генератор случайных чисел:** uz – тасодифий сонлар генератори en – random number generator	Алгоритм получения (выработки) случайных векторов (значений, чисел) с заданными вероятностными и алгебраическими характеристиками.
2.1.24	**генератор псевдослучайных чисел:** uz – псевдотасодифий сонлар генератори en – pseudorandom number generator	Алгоритм, генерирующий последовательность чисел, элементы которой почти независимы друг от друга и подчиняются заданному распределению.
2.1.25	**генерация ключа:** uz – калит генерацияси en – key generation	Процесс создания ключа.
2.1.26	**генератор ключей:** uz – калитлар генератори en – key generator	Криптографическое средство для выработки криптографических ключей или векторов инициализации
2.1.27	**группа:** uz – группа en – group	Множество элементов, на котором введена операция, обладающая свойством замкнутости, ассоциативности, наличием нейтрального элемента и обратного для каждого элемента группы.

O'zSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI

Термин	Определение
2.1.28 **дайджест сообщения:** uz – хабар дайжести en – message digest	Уникальная последовательность символов фиксированной длины, являющаяся результатом обработки данных с помощью односторонней хэш-функции, задаваемой определенным методом.
2.1.29 **данные:** uz – маълумотлар en – data	Информация, предоставленная в формализованном виде, пригодном для передачи, интерпретации или обработки с участием человека, либо автоматическими средствами.
2.1.30 **доступность информации:** uz – ахборотдан фойдалана олишлик en – information availability	Состояние информации и её носителя, при котором обеспечивается беспрепятственное и своевременное получение пользователями предназначенной для них информации.
2.1.31 **достоверность информации:** uz – ахборотнинг ишончлилиги en – information validity	Оценка вероятности отсутсвия ошибок в информации.
2.1.32 **допуск:** uz – фойдаланиш ҳуқуқи en – tolerance	Атрибут пользователя, разрешающий информационный доступ ко всей чувствительной информации заданного и более низких грифов секретности.
2.1.33 **загрузчик ключа:** uz – калит юкловчи en – key loader	Электронный автономный блок для хранения, по крайней мере, одного криптографического ключа и передачи его по запросу в оборудование.
2.1.34 **заявитель:** uz – даъво қилувчи en – declarant	Объект, который является принципалом или представляет его от имени этого объекта при аутентификационном обмене. Примечание – Заявитель выполняет функции, необходимые для обеспечения аутентификационного обмена от имени принципала.
2.1.35 **идентичность:** uz – айнан ўхшашлик en – identity	Уникальный системный признак, применяемый для пользователя.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT NAZORATINI MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARINI JORIY ETISH BOSHQARMASI

Термин	Определение
2.1.36 **имитостойкость шифра:** uz – шифрнинг имитобардошлилиги en – imitoresistance of cipher	Стойкость шифра к попыткам целенаправленного искажения шифротекста или навязывания ложной информации.
2.1.37 **информация:** uz – ахборот en – information	1 Сведения о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления. 2 Совокупность знаний, фактов, сведений, представляющих интерес и подлежащих хранению и обработке.
2.1.38 **информационная технология:** uz – ахборот технологияси en – information technology	Совокупность методов, устройств, способов и процессов, используемых для сбора, хранения, поиска, обработки и распространения информации.
2.1.39 **информационная система:** uz – ахборот тизими en – information system	Организационно упорядоченная совокупность информационных ресурсов, информационных технологий и средств связи, позволяющая осуществлять сбор, хранение, поиск, обработку и пользование информацией.
2.1.40 **код аутентификации сообщения:** uz – хабарни аутентификация қилиш коди en – message authentication code	Последовательность битов, являющаяся функцией обоих данных (открытого текста или шифротекста) и секретного ключа, которая присоединяется к данным, чтобы обеспечить аутентификацию данных.
2.1.41 **конфиденциальная информация:** uz – конфиденциал ахборот en – sensitive information	Документированная информация, доступ к которой ограничивается в соответствии с законодательством Республики Узбекис-тан.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Термин	Определение
2.1.42 конфиденциальность информации: uz – ахборотнинг конфиденциаллиги en – confidentiality of information	Состояние информации и её носителя, при котором обеспечиваются предотвращение несанкционированного ознакомления с ней или несанкционированного документирования (снятия копий).
2.1.43 корреляционная иммунность булевой функции: uz – буль функциясининг корреляцион бардошлилиги en – correlational immunity of Boolean function	Свойство булевой функции, заключающееся в сбалансированности всех частных функций, полученных из исходной функции фиксированием любых ее k и менее переменных.
2.1.44 лавинный эффект: uz - кўчки (лавина) эффекти en – avalanche effect	Свойство распространения влияния одного входного бита на многие выходные биты.
2.1.45 личные данные: uz – шахсий маълумотлар en – personal data	Любая информация, связанная с идентифицируемым лицом.
2.1.46 массив: uz – массив en – massive	Структура данных для представления множества элементов, однотипных по структуре и способу использования.
2.1.47 неотслеживаемость: uz – таъқиб эта олмаслик en – untracebility	Свойство, означающее невозможность получения противником и/или нарушителем сведений о действиях участников (протокола). Определяется для систем криптографических с большим количеством участников: систем платежей электронных, систем доступа к электронным информационным фондам и т.п.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Термин		Определение
2.1.48	**нелинейность булевой функции:** uz – буль функция чизиқсизлиги en – nonlinearity of Boolean function	Свойство булевой функции, показывающее степень удаленности булевой функции от множества аффинных и линейных булевых функций.
2.1.49	**перемешивание:** uz – аралаштириш en – mixing	Свойство шифрующего преобразования усложнять взаимосвязи между элементами данных, что затрудняет восстановление функциональных и статистических связей между открытым текстом, ключом и шифртекстом.
2.1.50	**перестановка:** uz – ўрин алмаштириш en – permutation	Одно из относительно простых криптографических преобразований открытого текста, при шифровании которого меняются местами друг с другом элементы (или их группы), по определенному правилу в пределах блока этого текста. При этом сами элементы остаются неизменными.
2.1.51	**подделка информации:** uz – ахборотни сохталаштириш en – data falsification	Умышленная несанкционированная модификация информации при ее передаче, хранении или обработке с целью получения определенных выгод перед конкурентом или нанесения ему ущерба.
2.1.52	**пользователь информации (потребитель информации):** uz – ахборот фойдаланувчиси (ахборот истеъмолчиси) en – information user (consumer)	Субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации (информационных продуктов) и пользующийся ею (ими).
2.1.53	**помехоустойчивость шифра:** uz – шифрнинг халақит бардошлилиги en – noise stability of a cipher	Способность шифра противостоять действию случайных помех (в отличие от целенаправленных действий противника), возникающих при передаче шифрованного сообщения по каналу связи.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT NAZORATINI MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARINI JORIY ETISH BOSHQARMASI

Термин		Определение
2.1.54	**последовательность случайных чисел:** uz - тасодифий сонлар кетма-кетлиги en – random number sequence	Последовательность чисел, каждое из которых не может быть предсказано (вычислено) только на основе знания предшествующих ему чисел данной последовательности.
2.1.55	**последовательность псевдослучайных чисел:** uz – псевдотасодифий сонлар кетма-кетлиги en – pseudo – random number sequence	Последовательность чисел, полученная в результате выполнения некоторого вычислительного процесса, используемая в конкретном случае вместо последовательности случайных чисел.
2.1.56	**подстановочный шифр:** uz – ўрнига қўйиш шифри en – substitution cipher	Способ шифрования путем замены одних символов (или битов) открытого текста другими символами (или битами).
2.1.57	**пороговая криптография:** uz – бўсағавий криптография en – threshold cryptography	Разбиение тайны (например, секретного ключа) на части таким образом, что только по некоторым подмножествам n частей можно восстановить тайну.
2.1.58	**предварительное распределение ключей:** uz – калитларни олдиндан тақсимлаш en – initial key distribution	Распределение не самих ключей, а некоторой меньшей по объему исходной информации, на основе которой в последствии каждая из сторон может вычислить ключ для взаимодействия с другой.
2.1.59	**пространство ключей:** uz – калитлар майдони en – field (spase) of keys	Множество всех ключей возможных для данной криптосистемы.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT NAZORATINI MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARINI JORIY ETISH BOSHQARMASI

Термин		Определение
2.1.60	**протокол:** uz – протокол en – protocol	1 Совокупность правил и соглашений, регламентирующих формат и процедуру передачи данных между двумя или несколькими независимыми устройствами или процессами. 2 Совокупность действий (инструкций, команд, вычислений, алгоритмов), выполняемых в заданной последовательности двумя или более субъектами с целью достижения определенного результата.
2.1.61	**протокол рукопожатия:** uz – қўл сиқишув протоколи en – handshake protocol	Протокол, позволяющий двум удаленным сторонам, владеющим некоторым общим секретом, осуществить взаимную проверку подлинности без раскрытия секрета.
2.1.62	**псевдослучайная последовательность:** uz – псевдотасодифий кетма-кетлик en – pseudorandom sequence	Последовательность чисел, которая была вычислена по некоторому определенному арифметическому правилу, но имеет все свойства случайной последовательности чисел в рамках решаемой задачи.
2.1.63	**псевдослучайные числа:** uz – псевдотасодифий сонлар en – pseudorandom numbers	Числа, которые получены по некоторому алгоритму, а используются как случайные.
2.1.64	**распределенный ключ:** uz – тақсимланган калит en – distributed key	Ключ, который разделен на некоторое количество частей и распределен между различными участниками. Примечание - К нему предъявляются два требования: оперативность и точность распределения, скрытность распределяемых ключей.
2.1.65	**расширение ключа:** uz – калитни кенгайтириш en – key extention	Создание из первоначального ключа другого ключа большего размера.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Термин		Определение
2.1.66	**режимы шифрования:** uz – шифрлаш режимлари en – modes of the cryptooperation	Методика, используемая в блочных шифрах, предотвращающая возможную утечку информации о повторяющихся частях шифруемых данных.
2.1.67	**режим электронной кодовой книги:** uz – электрон код китоби режими en – electronic code book (ECB) mode	Режим шифрования, в котором все блоки открытого текста шифруются независимо друг от друга на одном ключе в соответствии с алгоритмом шифрования данных.
2.1.68	**режим обратной связи по шифртексту:** uz – шифрматн бўйича тескари алоқа режими en – cipher feed back (CFB) mode	Режим шифрования, в котором блок открытого текста суммируется по модулю 2 с гаммой шифра. Вначале шифруется в режиме ECB вектор инициализации, затем результат шифрования суммируется по модулю 2 с первым блоком открытого текста и вновь подвергается шифрованию. В случае если последний блок неполный, используется только необходимое количество бит гаммы.
2.1.69	**режим обратной связи по выходу:** uz – чиқиш қийматлари бўйича тескари алоқа режими en – output feed back (OFB) mode	Режим шифрования, в котором вначале шифруется вектор инициализации, результат суммируется по модулю 2 с первым блоком открытого текста. После получения первого блока шифртекста, результат шифрования с предыдущего шага (до сложения) шифруется еще раз и складывается со следующим блоком открытого текста. В случае если последний блок неполный, используется только необходимое количество бит гаммы.
2.1.70	**совершенно нелинейная булевая функция (бент функция):** uz – мутлоқо чизиқсиз буль функцияси (бент функция) en – absolutely nonlinear Boolean function (bent function)	Булевая функция от n переменных, для которой расстояние Хэмминга до множества всех аффинных функций над векторным n-мерным пространством максимально и имеет постоянную величину.

O‘ZBEKISTON AXBOROT STANDARTLASHTIRISH, DAVLAT NAZORATINI MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARINI JORIY ETISH BOSHQARMASI

Термин	Определение
2.1.71 сообщение: uz – хабар en – message	1 Строка битов ограниченной длины. 2 Информация, выраженная в определенной форме и предназначенная для передачи от источника информации к ее получателю с помощью сигналов различной физической природы.
2.1.72 случайное число: uz – тасодифий сон en – random number	Число, выбранное из определенного набора чисел таким образом, что каждое число из данного набора может быть выбрано с одинаковой вероятностью.
2.1.73 ячейка: uz – ячейка en -cell	Минимальная адресуемая область оперативного запоминающего устройства или адресуемый элемент массива.
2.2 Защита информации	
2.2.1 защита информации: uz – ахборотни муҳофаза қилиш en – information protection	1 Совокупность методов и средств, обеспечивающих целостность, конфиденциальность, достоверность, аутентичность и доступность информации в условиях воздействия на нее угроз естественного или искусственного характера. 2 Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.
2.2.2 защищаемая информация: uz – муҳофаза қилинадиган ахборот en – protected information	Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации. Примечание – Собственником информации может быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Термин		Определение
2.2.3	**защита информации от утечки:** uz – ахборотни чиқиб кетишдан муҳофаза қилиш en – information protection from leak	Деятельность, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения, несанкционированного доступа к ней и получения защищаемой информации разведками.
2.2.4	**защита информации от несанкционированного воздействия:** uz – ахборотни рухсат этилмаган таъсирдан муҳофаза қилиш en - information protection from unauthorized action	Деятельность, направленная на предотвращение воздействия на защищаемую информацию с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.
2.2.5	**защита информации от несанкционированного доступа:** uz – ахборотни рухсатсиз фойдаланишдан муҳофаза қилиш en - information protection from unauthorized access	Деятельность, направленная на предотвращение получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации.
2.2.6	**защита информации от непреднамеренного воздействия:** uz - ахборотни қасддан қилинмаган таъсирдан муҳофаза қилиш en - information protection from inadvertent action	Деятельность, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации мероприятий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT NAZORATINI MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARINI JORIY ETISH BOSHQARMASI

Термин		Определение
2.2.7	**защита информации от разглашения:** uz - ахборотни ошкор этилишдан муҳофаза қилиш en - information protection from disclosure	Деятельность, направленная на предотвращение несанкционированного доведения защищаемой информации до потребителей, не имеющих права доступа к этой информации.
2.2.8	**защита информации от разведки:** uz - ахборотни разведкадан муҳофаза қилиш en - information protection from exploration	Деятельность, направленная на предотвращение получения защищаемой информации разведкой. Примечание – Получение защищаемой информации может быть осуществлено как иностранной, так и отечественной разведкой.
2.2.9	**мероприятие по защите информации:** uz - ахборотни муҳофаза қилиш тадбири en - measure protection of information	Совокупность действий, направленных на разработку и/или практическое применение способов и средств защиты информации.
2.2.10	**объект защиты информации:** uz - ахборотни муҳофаза қилиш объекти en - information protection object	Информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации.
2.2.11	**орган защиты информации:** uz – ахборотни муҳофаза қилиш органи en – authority of information protection	Административный орган, осуществляющий организацию защиты информации.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Термин		Определение
2.2.12	**организация защиты информации:** uz - ахборотни муҳофаза қилинишни ташкил этиш en - information protection development	Содержание и порядок действий, направленных на обеспечение защиты информации.
2.2.13	**показатель эффективности защиты информации:** uz - ахборотни муҳофаза қилиш самарадорлигининг кўрсаткичи en – efficiency of information protection indicator	Мера или характеристика для оценки эффективности защиты информации.
2.2.14	**режим сцепления блоков шифротекста:** uz – шифрматн блокларининг боғланиш режими en – cipher block chaining	Режим шифрования, в котором каждый зашифрованный (расшифрованный) блок криптографически зависит от предыдущего зашифрованного (расшифрованного) блока. Примечание - Для первого блока в качестве предыдущего блока шифртекста, используется вектор инициализации. В случае, если последний блок открытого текста неполный, он дополняется до необходимой длины.
2.2.15	**система защиты информации:** uz - ахборотни муҳофаза қилиш тизими en - information protection system	Совокупность органов и/или исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами в области защиты информации.
2.2.16	**согласование ключей:** uz – калитларни мувофиқлаштириш en – key agreement	Процесс, используемый двумя или несколькими сторонами, чтобы согласовать секретный симметричный ключ.

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT NAZORATINI MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARINI JORIY ETISH BOSHQARMASI

Термин		Определение
2.2.17	**составной шифр:** uz – қўшма (таркибли) шифр en – compound cipher	Шифр, составленный из нескольких более простых шифров.
2.2.18	**способ защиты информации:** uz - ахборотни муҳофаза қилиш усули en - information protection method	Порядок и правила применения определенных принципов и средств защиты информации.
2.2.19	**средство защиты информации:** uz - ахборотни муҳофаза қилиш воситаси en - information protection tools	Техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации (контроля эффективности защиты).
2.2.20	**средства имитозащиты:** uz – имитомуҳофаза воситалари en – imitoprotection means	Аппаратные, программные и аппаратно-программные средства, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации.
2.2.21	**средства кодирования:** uz – кодлаш воситалари en – coding tools	Средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций.
2.2.22	**срок безопасности:** uz – хавфсизлик муддати en –security period	Временной интервал, в течение которого криптографически защищенные данные имеют ценность.
2.2.23	**стойкость криптоалгоритма:** uz – криптоалгоритмнинг бардошлилиги en – stability of cryptoalgorithm	Способность криптоалгоритма противостоять всевозможным попыткам его раскрытия, т.е. атакам на него. Примечание - Стойкость определяется числом операций, необходимых для взлома криптосистем.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT NAZORATINI MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARINI JORIY ETISH BOSHQARMASI

Термин		Определение
2.2.24	**сцепление блоков:** uz –блокларни боғлаш en – block chaining	Шифрование информации таким образом, что каждый блок шифротекста криптографически зависим от предшествующего блока шифротекста.
2.2.25	**теория чисел:** uz – сонлар назарияси en – number theory	Раздел математики, изучающий натуральные числа и сходные объекты.
2.2.26	**традиционная криптография:** uz – анъанавий криптография en – traditional cryptography	Раздел криптографии, исследующий и разрабатывающий симметричные криптографические системы.
2.2.27	**уничтожение информации:** uz – ахборотни йўқ қилиш en – information destruction	Полная физическая ликвидация информации или ликвидация таких ее элементов, которые влияют на изменение существенных идентифицирующих информацию признаков.
2.2.28	**управление ключами:** uz – калитларни бошқариш en – key management	1 Совокупность мероприятий и процедур, обеспечивающих защищенную генерацию, распределение, хранение и уничтожение ключей. 2 Действия, выполняемые в течение полного цикла жизни ключей, включающие управление криптографическими ключами и другими параметрами, связанными с безопасностью (например, векторы инициализации и пароли), а также их генерацию, хранение, установку, ввод, вывод и обнуление.
2.2.29	**уполномоченный орган:** uz – ваколатли орган en – representative authority	Орган, осуществляющий единую государственную политику и обеспечивающий проведение сертификации продукции (услуг) в области криптографической защиты информации.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Термин		Определение
2.2.30	**уравнение зашифрования:** uz – шифрлаш тенгламаси en – ciphering function	Соотношение, выражающее процесс образования зашифрованных данных из открытых данных в результате преобразований, заданных алгоритмом криптографического преобразования.
2.2.31	**уравнение расшифрования:** uz – дастлабки матнга ўгириш тенгламаси en – deciphering function	Соотношение, выражающее процесс образования открытых данных из зашифрованных данных в результате преобразований, заданных алгоритмом криптографического преобразования.
2.2.32	**функция-ловушка:** uz – тузоқ функция en – function-trap	Одностороння функция, для которой обратную функцию вычислить просто, если имеется некоторая дополнительная информация, и сложно, если такая информация отсутствует.
2.2.33	**хранение ключа:** uz – калитни сақлаш en – keeping of the key	Процедуры, необходимые для хранения ключа в надлежащих условиях, обеспечивающих его безопасность до момента его замены.
2.2.34	**цель защиты информации:** uz – ахборотни муҳофаза қилиш мақсади en – purpose of information protection	Заранее намеченный результат защиты информации. Примечание – Целью защиты информации может быть предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на информацию.
2.2.35	**центр доверия:** uz – ишонч маркази en –trusted centre	Особый участник протокола криптографиического, которому доверяют все остальные его участники, введенный в протокол для усиления его безопасности. Примечание - Различают следующие виды центра доверия: центр регистрации, центр распределения ключей, центр сертификации, центр установки меток временных, центр нотаризации и т.д.
2.2.36	**центр распределения ключей:** uz – калитларни тақсимлаш маркази en – key distribution centre	Система, уполномоченная передавать временные сеансовые ключи доверителям. Примечание – Каждый сеансовый ключ передается в шифрованном виде, для чего используется главный ключ, применяемый центром распределения ключей совместно с доверителем, которому передаются данные.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT NAZORATINI MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARINI JORIY ETISH BOSHQARMASI

Термин		Определение
2.2.37	**цикл жизненный ключей:** uz –калитларнинг ҳаётий цикли en – key lifetime	Последовательность стадий, которые проходят ключи от момента генерации до момента уничтожения. Примечание – Включает такие основные стадии, как: генерация, регистрация ключей (и пользователей), инициализация, период действия, хранение, смена, архивирование, уничтожение и восстановление.
2.2.38	**цифровой отпечаток:** uz – рақамли из en – digital imprint	Характеристика элемента данных, такая как криптографическое контрольное число или результат применения к данным односторонней функции; в значительной степени индивидуальна для элемента данных, при этом вычислительно невозможно найти другой элемент данных, обладающий такой же характеристикой.
2.2.39	**экспорт шифрования:** uz – шифрлаш экспорти en - export of cryptooperation	Шифрование в любой форме, которое вывозится из страны-производителя: например, зашифрованная информация или компьютерный диск, содержащий алгоритмы шифрования.
2.2.40	**эффективность защиты информации:** uz - ахборотни муҳофаза қилиш самарадорлиги en – efficiency of information Protection	Степень соответствия результатов защиты информации поставленной цели.
2.3 Криптология		
2.3.1	**депонирование ключей:** uz – калитларни сақлаш учун топшириш en – key escrow	Хранение копии ключа криптосистемы у доверенного лица (организации, участника протокола и т.п.) с целью восстановления работоспособности криптосистемы, например, в случае утери ключа.

O'ZBEKISTON STANDARTLASHTIRISH, DAVLAT NAZORATINI MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARINI JORIY ETISH BOSHQARMASI AGENTLIGI

Термин		Определение
2.3.2	**обновление ключей:** uz – калитларни янгилаш en – key updating	Способ смены ключей, при котором новый ключ генерируется с помощью вычисления значения функции (обычно функции однонаправленной) от аргумента, определяемого предыдущим ключом и, возможно, другими данными.
2.3.3	**криптология:** uz – криптология en – cryptology	Наука (отрасль знаний), изучающая криптографические преобразования, которая включает в себя два направления – криптографию и криптоанализ.
2.3.4	**криптография:** uz – криптография en – cryptography	Научная дисциплина (отрасль знаний), изучающая принципы, средства и методы преобразования информации с целью защиты содержания информации от несанкционированного доступа, предотвращение возможности ее искажения.
2.3.5	**криптограф:** uz – криптограф en – cryptographer	Специалист в области криптографии.
2.3.6	**криптоаналитик:** uz – криптотаҳлилчи en – cryptanalyst	Специалист, занимающийся криптоанализом.
2.3.7	**криптографический протокол:** uz – криптографик протокол en – cryptographic protocol	1 Набор правил и процедур, определяющих использование криптоалгоритма и ключей шифрования. 2 Протокол, предусматривающий взаимодействие двух и более сторон с использованием криптографических алгоритмов.
2.3.8	**криптостойкость; криптографическая стойкость:** uz – криптобардошлилик, криптографик бардошлилик en – cryptographic strength	1 Устойчивость криптографического алгоритма к его криптоанализу. 2 Способность криптосистемы выдерживать различные нападения. Примечание - Количественно выражается числом операций некоторого типа, которые необходимо выполнить для решения задачи криптоанализа.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Термин	Определение
2.3.9 криптосистема с открытым ключом (асимметричная криптосистема): uz – очиқ калитли криптотизим (асимметрик криптотизим) en – cryptosystem with public key	Криптографическая система, в которой используются два ключа: секретный и открытый, причем ни один из ключей не может быть вычислен из другого за приемлемое время. Примечание - Секретный ключ должен содержаться в тайне, в то время как открытый ключ может быть разослан всем абонентам, с которыми осуществляется взаимодействие.
2.3.10 криптографическая защита информации: uz – ахборотни криптографик муҳофаза қилиш en – cryptographic protection to information	Комплекс мероприятий, направленных на обеспечение целостности, доступности и конфиденциальности информации, осуществляемых при помощи алгоритмов криптографического преобразования (криптоалгоритмов).
2.3.11 криптографическая защита: uz - криптографик муҳофаза қилиш en – cryptographic protection	1 Защита информационных процессов от целенаправленных попыток отклонить их от нормальных условий протекания, базирующаяся на криптографических преобразованиях данных. 2 Защита информации от несанкционированного доступа и изменения при помощи алгоритмов криптографического преобразования. Примечание - Для криптографической защиты в системах удаленного банковского обслуживания используется электронная цифровая подпись и шифрование передаваемой информации.
2.3.12 ключ (криптографический) uz – калит (криптографик) en – key (cryptographic)	1 Конкретное секретное состояние некоторого набора параметров криптографического алгоритма, обеспечивающее выбор одного преобразования из совокупности возможных для данного алгоритма преобразований. 2 Общее название открытых и секретных ключей асимметричных криптосистем; представляют собой последовательность символов, применяемую для вычисления или проверки электронной цифровой подписи, а также для шифрования и расшифрования.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT NAZORATINI MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARINI JORIY ETISH BOSHQARMASI

Термин	Определение
2.3.13 **ключевое отношение:** uz –калитли муносабат en – key relations	Состояние, существующее между связующейся парой, в течение которого они совместно владеют, по крайней мере, одним ключом данных.
2.3.14 **ключевой материал:** uz –калитли маълумот en – key material	Данные (например, ключи и инициализирующие значения), необходимые для установления и ведения ключевого отношения.
2.3.15 **компонент ключа:** uz –калит компоненти en – key component	Один из двух или нескольких параметров, имеющий формат криптографического ключа и объединяемый с одним или несколькими подобными параметрами путем сложения по модулю 2 для формирования криптографического ключа.
2.3.16 **криптопериод:** uz –криптодавр en –cryptoperiod	Временной интервал, в течение которого разрешено использование определенного ключа, либо в течение которого могут действовать ключи для данной системы.
2.3.17 **криптографический метод защиты информации:** uz – ахборотни муҳофаза қилишнинг криптографик усули en – cryptographic method of information protection	Метод защиты информации, основанный на принципах шифрования и/или электронной цифровой подписи. Примечание - Криптографический метод может быть реализован программными, аппаратными и аппаратно-программными средствами.
2.3.18 **криптографическое преобразование:** uz – криптографик алмаштириш en – cryptographic transformation	1 Преобразование данных по криптографическому алгоритму, в котором часть параметров держится в секрете. 2 Процедура специального преобразования информации для решения одной из следующих криптографических задач: шифрования данных, хэширования данных или формирования электронной цифровой подписи, имитовставки, вычисления специальных криптографических контрольных сумм.

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Термин	Определение
2.3.19 криптографические примитивы: uz – криптографик примитивлар en – cryptographic primitives	Элементарные действия по обработке информации, в том числе с использованием криптографического ключа, совокупность применения которых в определенной последовательности является алгоритмом шифрования.
2.3.20 криптографическая синхронизация: uz –криптографик синхронлаш en – cryptographic synchronization	Согласование процесса шифрования и дешифрования.
2.3.21 криптографическая система (криптосистема): uz – криптографик тизим (криптотизим) en – cryptographic system (cryptosystem)	Совокупность организационных, технических и программных средств, обеспечивающих криптографическое преобразование информации и/или управление, в том числе автоматизированное, процессом изготовления и распределения криптографиических ключей.
2.3.22 симметричная криптосистема (криптосистема с секретным ключом): uz – симметрик криптотизим (махфий калитли криптотизим) en – symmetric cryptosystem, (cryptosystem with private key)	Криптографическая система, в которой один и тот же криптографический ключ используется для зашифрования и расшифрования информации. Примечание – Такие криптосистемы также называются симметричными, одноключевыми или классическими.
2.3.23 стеганография: uz – стеганография en – steganography	Отрасль науки, изучающая математические методы сокрытия конфиденциальной информации в открытых информационных массивах.
2.3.24 энтропия: uz – энтропия en – entropy	Мера неопределенности источника сообщений, определяемая вероятностями появления тех или иных символов при их передаче.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT NAZORATINI MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARINI JORIY ETISH BOSHQARMASI

Термин	Определение
2.3.25 **экспоненциальное время:** uz – экспоненциал вақт en – exponential time	Сложность алгоритма, которая экспоненциально зависит от длины параметра (например, длины ключа).

2.4 Криптографические алгоритмы

2.4.1 **алгоритм аутентификации пользователя:** uz – фойдаланувчини аутентификация қилиш алгоритми en – user autentification algorithm	Последовательность действий, которая известна пользователю или содержится в устройстве доступа. Примечание - Он используется для защищенного доступа к услуге.
2.4.2 **алгоритм шифрования данных:** uz – маълумотларни шифрлаш алгоритми en – data encryption algorithm	Криптографический алгоритм по преобразованию исходного текста к зашифрованному тексту и/или наоборот, определяющий содержание и последовательность операций, зависящих от ключевой переменной (ключ шифрования).
2.4.3 **алгоритм электронной цифровой подписи:** uz – электрон рақамли имзо алгоритми en – electronic digital signature algorithm	Криптографический алгоритм, предназначенный для формирования и подтверждения подлинности электронной цифровой подписи под заданным сообщением (электронным документом), передаваемым по незащищенным телекоммуникационным каналам общего пользования.
2.4.4 **алгоритм хэширования:** uz – хэшлаш алгоритми en – hashing algorithm	Криптографический алгоритм, преобразующий исходную последовательность битов конечной длины в последовательность битов фиксированной длины.
2.4.5 **асимметричный шифр** uz – асимметрик шифр en – asymmetric cipher	Шифр, в котором секретный ключ шифрования не совпадает с открытым ключом расшифрования и является трудно вычислимым на основе открытого ключа.

O ‘zSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT NAZORATINI MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARINI JORIY ETISH BOSHQARMASI

Термин		Определение
2.4.6	**асимметричное шифрование:** uz – асимметрик шифрлаш en – asymmetric encryption	Метод, при котором для шифрования и расшифрования применяются разные ключи, один из которых трудно вычислить на основе другого.
2.4.7	**блочный алгоритм шифрования; блочный шифр:** uz - блокли шифрлаш алгоритми; блокли шифр en – block ciphering algorithm, block cipher	1 Алгоритм шифрования, осуществляющий криптографическое преобразование исходной информации путем выполнения криптографических операций над n-битными блоками исходного или зашифрованного текста. 2 Шифр, входными текстами для которого являются блоки фиксированного размера.
2.4.8	**дискретный логарифм:** uz – дискрет логарифм en – discrete logarithm	Целочисленный показатель степени, в которую нужно возвести некоторый элемент конечного поля, чтобы вычислить другой.
2.4.9	**коммутативность:** uz – коммутативлик en – commutativety	Независимость результата операции от порядка операндов.
2.4.10	**конкатенация:** uz – конкатенация en – concatenation	Соединение последовательностей символов.
2.4.11	**криптографический алгоритм (криптоалгоритм); алгоритм криптографического преобразования:** uz - криптографик алгоритм; криптографик алмаштириш алгоритми en – cryptographic algorithm	1 Математический алгоритм преобразования информации (данных) с целью предотвратить возможность её искажения и защитить от несанкционированного доступа. 2 Алгоритм преобразования данных, использующий в своей работе набор секретных и открытых параметров, публикуемый, как правило, в открытой печати.

© O‘ZBEKISTON AGENTLIGI STANDARTLASHTIRISH, DAVLAT NAZORATINI MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARINI JORIY ETISH BOSHQARMASI

	Термин	Определение
2.4.12	**криптосистема эллиптической кривой (ECC):** uz – эллиптик эгри чизиқли криптотизим en – elliptic curve cryptosystem	Асимметричная криптосистема, основанная на свойствах эллиптических кривых. Примечание - Например, структура группы может быть задана точками эллиптической кривой и для такой группы можно сформулировать проблему дискретного логарифма. Эта проблема считается жесткой и потому может быть использована для создания криптосистемы
2.4.13	**метод решета в числовом поле:** uz – сонли майдонда панжара усули en – number field sieve	Общий алгоритм факторизация чисел, считающийся наиболее эффективным.
2.4.14	**метод Полларда:** uz – Поллард усули en – Pollard method	Алгоритм поиска простого делителя p целого числа n, основанный на анализе свойств чисел p-1 и p+1.
2.4.15	**метод Полларда-Ро:** uz – Поллард– Ро усули en – Pollard Rho method	Алгоритм решения задачи дискретного логарифмирования, в том числе на эллиптической кривой.
2.4.16	**поле Галуа:** uz – Галуа майдони en – Galois field	Поле, состоящее из конечного множества элементов.
2.4.17	**проблема дискретного логарифма:** uz – дискрет логарифм муаммоси en - discrete logarithm problem	Математическая задача поиска логарифма в больших конечных полях.
2.4.18	**проблема дискретного логарифма на эллиптической кривой (ECDL):** uz – эллиптик эгри чизиқли дискрет логарифм муаммоси en – elliptic curve discrete logarithm (ECDL) problem	Поиск числа m, удовлетворяющего условию mP = Q, где P и Q – точки с x- и y- координатами на эллиптической кривой.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT NAZORATINI MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARINI JORIY ETISH BOSHQARMASI

Термин		Определение
2.4.19	**разложение на множители методом эллиптической кривой:** uz – эллиптик эгри чизиқ усулида туб кўпайтувчиларга ажратиш en – elliptic curve (factoring) method	Специальный алгоритм разложения на множители с целью найти главный фактор p сложного целого числа n методом нахождения эллиптической кривой, количество точек которой, имеющих модуль p, делится только на меньший фактор.
2.4.20	**симметричный шифр** uz – симметрик шифр en – symmetric cipher	Шифр, являющийся симметричной криптографической системой, то есть использующий для зашифрования и расшифрования один и тот же ключ или такие различные ключи, что по одному из них легко может быть получен другой.
2.4.21	**симметричное шифрование:** uz – симметрик шифрлаш en – symmetric encryption	Шифрование с использованием одного и того же ключа как для зашифрования, так и для расшифрования информации.
2.4.22	**факторизация:** uz – туб кўпайтувчиларга ажратиш (факторлаштириш) en – factoring	Разложение целого числа на простые множители.
2.4.23	**фактор:** uz – фактор en – factor	Простой делитель; для любого целого числа n фактором является простое число, на которое n делится без остатка. Примечание - Например, 7 – фактор числа 91, потому что результат деления 91 на 7 является целым числом и 7-простое число.
2.4.24	**эллиптическая кривая:** uz – эллиптик эгри чизиқ en – elliptic curve	Множество точек (x,y), удовлетворяющих уравнению $y^2 = x^3 + ax + b$ в конечном простом поле.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Термин	Определение

2.5 Электронная цифровая подпись (ЭЦП)

2.5.1	**бесконфликтность:** uz – зиддиятсизлик en – collision-free	Хэш-функция является бесконфликтной, если коллизии сложно обнаружить.
2.5.2	**владелец закрытого ключа ЭЦП:** uz – ЭРИ ёпиқ калитининг эгаси en – owner of private key of the EDS	Физическое лицо, создавшее ЭЦП (подписывающее электронный документ) и на имя которого центром регистрации выдан сертификат ключа ЭЦП.
2.5.3	**дополнение:** uz – тўлдирувчи en - appendix	Строка бит, формируемая из ЭЦП и произвольного текстового поля.
2.5.4	**закрытый ключ ЭЦП:** uz – ЭРИнинг ёпиқ калити en – private key of EDS	Последовательность символов, полученная с использованием средств ЭЦП, известная только подписывающему лицу и предназначенная для создания ЭЦП в электронном документе.
2.5.5	**инфраструктура открытых ключей:** uz – очиқ калитлар инфратузилмаси en – public key infrastructure, PKI	Техническая и организационная инфраструктура, которая обеспечивает поддержку использования технологий криптопреобразований с открытым ключом. Примечание – Инфраструктура открытых ключей должна поддерживать технологию распространения цифровых сертификатов: выдачу и аннулирование сертификатов, хранение информации, необходимой для последующей проверки подлинности сертификатов.
2.5.6	**ключ обнаружения подделки ЭЦП:** uz – ЭРИнинг сохталаштирилганлигини аниқлаш калити en – falsification detection key EDS	Пара целых чисел, используемая в процессе подтверждения подлинности ЭЦП.
2.5.7	**ключ хэширования:** uz – хэшлаш калити en – hashing key	Последовательность символов фиксированной длины, обеспечивающая выбор одного преобразования из совокупности всевозможных для алгоритма криптографического преобразования данных.

O ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Термин		Определение
2.5.8	**коллизия:** uz – коллизия en – collision	Событие, соответствующее тому, что значения односторонней функции для двух различных исходных данных совпадают.
2.5.9	**контрольный ключ:** uz – назорат калити en – control key	Первая компонента ключа обнаружения подделки ЭЦП, генерируемая в виде случайного или псевдослучайного числа.
2.5.10	**однонаправленная функция:** uz – бир томонлама функция en – one-way function	Функция, для которой по заданному аргументу x легко вычислить значение функции f (x), тогда как определение x из f (x) трудно вычислимо.
2.5.11	**открытый ключ ЭЦП:** uz – ЭРИнинг очиқ калити en – public key of EDS	Последовательность символов, полученная с использованием средств ЭЦП, соответствующая закрытому ключу ЭЦП, доступная любому пользователю информационной системы и предназначенная для подтверждения подлинности ЭЦП в электронном документе.
2.5.12	**отправитель электронного документа:** uz – электрон ҳужжатни жўнатувчи en – sender of the electronic document	Юридическое или физическое лицо, указанное в реквизитах электронного документа и отправляющее электронный документ получателю электронного документа.
2.5.13	**параметр алгоритма ЭЦП:** uz – ЭРИ алгоритмининг параметри en – parameter of algorithm of EDS	Элемент данных, общий для всех субъектов алгоритма ЭЦП, известный или доступный всем этим субъектам.
2.5.14	**пластиковая карта:** uz – пластик карта en – plastic card	Персонализированный платежный инструмент, предоставляющий пользующемуся картой лицу возможность безналичной оплаты товаров и услуг, а также получения наличных средств в отделениях банковучастников платежной системы и банкоматах.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT NAZORATINI MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARINI JORIY ETISH BOSHQARMASI

Термин		Определение
2.5.15	**подписанное сообщение:** uz – имзоланган хабар en – signed message	Набор элементов данных, состоящий из сообщения и дополнения, содержащего наряду с ЭЦП идентификаторы субъекта, подписавшего сообщение, и/или метку времени.
2.5.16	**пользователь открытого ключа ЭЦП:** uz – ЭРИ очиқ калити фойдаланувчиси en – public key user EDS	Юридическое или физическое лицо, использующее открытый ключ ЭЦП для подтверждения подлинности ЭЦП.
2.5.17	**получатель электронного документа:** uz – электрон ҳужжатни олувчи en – receiver of electronic document	Юридическое или физическое лицо, которому электронный документ адресован отправителем электронного документа.
2.5.18	**подтверждение подлинности ЭЦП:** uz – ЭРИнинг ҳақиқий-лигини тасдиқлаш en – authentication of EDS	Положительный результат проверки принадлежности ЭЦП владельцу закрытого ключа ЭЦП и отсутствия искажений информации в электронном документе.
2.5.19	**процесс формирования ЭЦП и сеансового ключа:** uz – ЭРИ ва сеанс калитини шакллантириш жараёни en – signature and session key processes EDS	Процесс, в качестве исходных данных которого используются контрольный ключ (только для режима с сеансовым ключом), сообщение, закрытый ключ ЭЦП и параметры алгоритма ЭЦП (АЭЦП), а в результате формируется ЭЦП и сеансовый ключ (только для режима с сеансовым ключом).

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT NAZORATINI MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARINI JORIY ETISH BOSHQARMASI

Термин		Определение
2.5.20	**процесс подтверждения подлинности ЭЦП:** uz – ЭРИнинг ҳақиқийлигини тасдиқлаш жараёни en – verification processes EDS	Процесс, в качестве исходных данных которого используются ключ обнаружения подделки ЭЦП (только для режима с сеансовым ключом), подписанное сообщение, открытый ключ ЭЦП и параметры АЭЦП, результатом которого является заключение о подлинности или неподлинности ЭЦП.
2.5.21	**реквизиты электронного документа:** uz – электрон ҳужжат реквизитлари en – electronic documents attributes	Обязательные сведения (ЭЦП, наименование юридического лица или фамилия, имя, отчество физического лица-отправителя электронного документа, почтовый и электронный адрес отправителя электронного документа, дата его создания), которые должны содержаться в электронном документе для признания его действительным.
2.5.22	**свидетельство:** uz – гувоҳнома en – witness	Элемент данных, представляющий соответствующее доказательство подлинности (неподлинности) ЭЦП проверяющей стороне.
2.5.23	**сеансовый ключ ЭЦП:** uz – ЭРИнинг сеанс калити en – session key EDS	Вторая компонента ключа обнаружения подделки ЭЦП, функционально связанная с первой компонентой последнего, закрытым ключом ЭЦП и ЭЦП.
2.5.24	**секретный ключ:** uz – махфий калит en – private key	Криптографический ключ, принадлежащий и известный только лицу, сформировавшему при помощи этого ключа криптографические преобразования.
2.5.25	**сертификат ключа ЭЦП:** uz – ЭРИ калити сертификати en – certificate for public key EDS	Документ, подтверждающий соответствие открытого ключа ЭЦП закрытому ключу ЭЦП и выданный Центром регистрации владельцу закрытого ключа ЭЦП.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT NAZORATINI MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARINI JORIY ETISH BOSHQARMASI

	Термин	Определение
2.5.26	**сертификат на средство ЭЦП:** uz – ЭРИ воситаси сертификати en – certificate for EDS means	Документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств ЭЦП установленным требованиям безопасности.
2.5.27	**слепая подпись:** uz – кўр-кўрона имзо en – blind signature	Протокол формирования ЭЦП, позволяющий сформировать правильную ЭЦП, соответствующую некоторому зашифрованному цифровому сообщению.
2.5.28	**средства ЭЦП:** uz – ЭРИ воситалари en – facilities EDS	Совокупность технических и программных средств, обеспечивающих создание ЭЦП в электронном документе, подтверждение подлинности ЭЦП, создание открытых и закрытых ключей ЭЦП.
2.5.29	**участник электронной коммерции:** uz – электрон тижорат иштирокчиси en – participant of electronic commerce	Юридические и физические лица, осуществляющие электронную коммерцию, а также юридические и физические лица, являющиеся покупателями соответствующих товаров (работ, услуг).
2.5.30	**функция сжатия:** uz – зичлаш функцияси en – compression function	Функция, которая преобразует код определенной длины в более короткий код.
2.5.31	**хэш, хэш-значение:** uz – хэш, хэш-қиймат en – hash, hash-value	Число, вырабатываемое из последовательности данных, и генерируемое таким образом, чтобы сделать маловероятным получение такого же значения из других входных данных.
2.5.32	**хэш-код:** uz – хэш-код en – hash-code	Строка бит, являющаяся выходным результатом хэш-функции.

O`ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Термин	Определение
2.5.33 хэширование: uz – хэшлаш en – hashing	1 Процесс вычисления значения хэш-функции. 2 Преобразование массива данных произвольного размера в блок данных фиксированного размера, служащий заменителем исходного массива в некоторых контекстах.
2.5.34 хэш-функция (функция хэширования): uz – хэш-функция (хэшлаш функцияси) en – hash-function	1 Функция, отображающая строки бит конечной длины в строки бит фиксированной длины. 2 Математическое преобразование массива данных произвольного размера и вычисление для него фиксированной уникальной последовательности небольшой длины.
2.5.35 центр регистрации ключей ЭЦП: uz – ЭРИ калитларини рўйхатга олиш маркази en – center of EDS keys registration	1 Юридическое лицо, прошедшее государственную регистрацию в специально уполномоченном органе и выполняющее функции, предусмотренные законодательством. 2 Юридическое лицо, обладающее правомочиями на удостоверение принадлежности конкретного ключа ЭЦП.
2.5.36 электронная цифровая подпись, ЭЦП: uz – электрон рақамли имзо, ЭРИ en – electronic digital signature, EDS	Подпись в электронном документе, полученная в результате специальных преобразований информации данного электронного документа с использованием закрытого ключа ЭЦП и позволяющая при помощи открытого ключа ЭЦП установить отсутствие искажения информации в электронном документе и идентифицировать владельца закрытого ключа ЭЦП.
2.5.37 электронный документ: uz – электрон ҳужжат en – electronic document	Информация, зафиксированная в электронной форме, подтвержденная ЭЦП и имеющая другие реквизиты электронного документа, позволяющие его идентифицировать.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT NAZORATINI MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARINI JORIY ETISH BOSHQARMASI

Термин		Определение
2.5.38	**электронный документооборот:** uz – электрон ҳужжат айланиши en – electronic documents circulation	Совокупность процессов отправки и получения электронных документов через информационную систему.
2.5.39	**электронные деньги:** uz – электрон пуллар en – electronic money, e-money	Деньги, существующие в виде специальных записей в компьютере или интеллектуальной карте, которые используются для покупок и взаиморасчетов контрагентов в рамках конкретной информационной технологии.
2.5.40	**электронная коммерция:** uz – электрон тижорат en – electronic commerce	Предпринимательская деятельность по продаже товаров, выполнению работ и оказанию услуг, осуществляемая с использованием информационных систем.
2.5.41	**электронный платёж:** uz – электрон тўлов en – electronic payment	Платёж, проводимый с помощью электронного платежного документа в соответствии с законодательством и установленными процедурами.
2.5.42	**этапный ключ хэширования:** uz – хэшлашнинг босқич калити en – hashing round key	Функция от ключа хэширования и промежуточного результата хэширования.
2.6 Шифрование		
2.6.1	**абонентское шифрование:** uz – абонент шифрлаш en – subscriber encryption	Криптографическое преобразование с целью защиты информации, передаваемой между двумя субъектами автоматизированной системы.

O'ZBEKISTON AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

	Термин	Определение
2.6.2	**вероятностное шифрование:** uz – эҳтимолий шифрлаш en – probabilistic encryption	1 Схема шифрования, в которой одному открытому тексту может соответствовать множество шифротекстов. 2 Процесс шифрования с использованием случайных параметров.
2.6.3	**гибкий шифр:** uz – мослашувчан шифр en – flexible cipher	Шифр, описываемый как набор крипто-алгоритмов, выбираемых в зависимости от секретного ключа.
2.6.4	**дешифрование:** uz – шифрни калитсиз очиш (дешифрлаш) en – decryption	Процесс криптоанализа, завершающийся с восстановлением исходного текста из зашифрованного без знания ключа шифрования.
2.6.5	**диаматрица:** uz – диаматрица en – diamatrix	Квадратная матрица, образованная как результат диапреобразования другой квадратной матрицы.
2.6.6	**диаминор:** uz – диаминор en – diaminor	Имя функции, используемой в процессе обращения диаматрицы.
2.6.7	**диапреобразование:** uz – диаалмаштириш en – diatransformation	Преобразование квадратной матрицы U в новую квадратную матрицу dU того же порядка, удовлетворяющее следующим условиям: всякий элемент главной диагонали матрицы dU равен сумме элементов соответствующего столбца матрицы U, а всякий недиагональный элемент матрицы dU равен соответствующему элементу матрицы U взятому с противоположным знаком. При этом матрицу dU называют диаматрицей матрицы U.
2.6.8	**диаопределитель диаматрицы:** uz – диаматрица диааниқловчиси en – diadeterminant of the diamatrix	Число, равное по значению определителю матрицы, на основе которой сформирована упомянутая диаматрица как результат диапреобразования.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

	Термин	Определение
2.6.9	**зашифрование данных:** uz – маълумотларни шифрматнга ўгириш en – enciphering data	Процесс преобразования исходных данных в зашифрованные при помощи шифра.
2.6.10	**имитозащита:** uz – имитомуҳофаза en – imitational protection	Защита системы шифрованной связи от навязывания ложных данных.
2.6.11	**имитовставка:** uz – имитоқўшимча en – digital timestamp	Отрезок информации фиксированной длины, полученный по определенному правилу из открытых данных и секретного ключа и добавленный к зашифрованным данным для обеспечения имитозащиты.
2.6.12	**инициализирующее (начальное) значение:** uz – инициализация-ловчи (бошланғич) қиймат en – initial value	Значение, используемое для установления начальной точки процесса шифрования.
2.6.13	**канальное шифрование:** uz – каналли шифрлаш en – channel encryption	Вид защиты информации в каналах связи между узлами на основе шифрования всех данных, включая открытый текст и информацию о его маршрутизации и коммуникационном протоколе, где узлы могут быть промежуточными на пути от отправителя к получателю.
2.6.14	**ключ шифрования:** uz – шифрлаш калити en – encryption key	Секретный криптографический ключ шифра.
2.6.15	**обратная диаматрица:** uz – тескари диаматрица en – reverse diamatrix	Квадратная матрица, обратная по отношению к диаматрице.
2.6.16	**обратная матрица:** uz – тескари матрица en – reverse matrix	Квадратная матрица, обратная по отношению к матрице.

© O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Термин		Определение
2.6.17	**полубайт:** uz – яримбайт en – nibble (halfbyte)	Единица измерения информации в четыре бит.
2.6.18	**потоковый шифр:** uz – оқимли (узлуксиз) шифр en – stream cipher	Шифр, преобразующий последовательно отдельные биты или знаки открытого текста и ориентированный на реализацию в виде программы.
2.6.19	**расшифрование данных:** uz – маълумотларни дастлабки матнга ўгириш en – deciphering data	Процесс преобразования зашифрованных данных в исходные при помощи шифра.
2.6.20	**раунд или цикл шифрования:** uz – шифрлаш раунди ёки цикли en – period or cycle of ciphering	Один комплексный шаг шифрования, в ходе которого одна или несколько частей шифруемого блока данных подвергаются модификации.
2.6.21	**режим шифрования со счетчиком:** uz – ҳисоблагич бўйича шифрлаш режими en – counter (CTR) mode	Режим шифрования, в котором для зашифрования/расшифрования результат шифрования блока счетчика суммируется по модулю 2 с открытым текстом/шифротекстом.
2.6.22	**сеансово-этапный ключ:** uz – сеанс-босқич калити en – phase-session key	Секретный ключ, являющийся функцией ключа шифрования и функционального ключа.
2.6.23	**состояние:** uz – ҳолат en – state	Промежуточный результат криптографического преобразования.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Термин		Определение
2.6.24	**средства шифрования:** uz – шифрлаш воситалари en – facilities of the cryptooperation	Аппаратные, программные и аппаратно-программные средства, реализующие криптографические алгоритмы преобразования информации и предназначенные для защиты информации от несанкционированного доступа при ее обработке, хранении и передаче по каналам связи.
2.6.25	**функция криптографическая:** uz – криптографик функция en – cryptographic function	Функция, необходимая для реализации криптографической системы. Примечание – К таким функциям относятся: генерация ключей, генерация псевдослучайных последовательностей, функция шифрования, вычисление и проверка значений кода аутентичности сообщения и цифровой подписи, вычисление значения хэш-функции и др.
2.6.26	**функция шифрования:** uz – шифрлаш функцияси en – encryption function	Функция, используемая в шифре для преобразования данных с применением ключа.
2.6.27	**функциональный ключ:** uz – функционал калит en – functional key	Секретный ключ, являющийся функцией ключа шифрования или формируемый независимо от ключа шифрования.
2.6.28	**шифрование сеанса:** uz – шифрлаш сеанси en – session encryption	Способ реализации сеанса связи между двумя сторонами, при котором все передаваемые в процессе его выполнения сообщения шифруются на специально сгенерированном для данного сеанса ключе.
2.6.29	**шифр**: uz – шифр en – cipher	Совокупность обратимых преобразований множества возможных открытых (исходных) данных на множество возможных зашифрованных данных, осуществляемых по определенным правилам с применением ключей.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Термин	Определение
2.6.30 шифр совершенный: uz – такомиллашган шифр en – perfect cipher	Шифр, при использовании которого шифрованный текст не дает противнику, не знающему секретного ключа, никакой информации об открытом тексте, т.е. условное распределение на множестве открытых текстов при заданном шифрованном тексте совпадает с безусловным распределением на множестве открытых текстов.
2.6.31 шифртекст, зашифрованный текст: uz – шифр матн, шифрланган матн en – ciphertext, enciphered text	Результат зашифрования исходного открытого текста, осуществляемого с целью сокрытия его смысла.
2.6.32 шифрование с открытым ключом: uz – очиқ калитли шифрлаш en – public key encryption	Криптографический метод, в котором используется открытый ключ для формирования шифротекста и закрытый ключ для преобразования шифротекст в исходный текст.
2.6.33 шифрование информации: uz – ахборотни шифрлаш en – information encryption	Процесс преобразования открытых данных в зашифрованные с помощью шифра.
2.6.34 этап: uz – босқич en – round	Однотипная совокупность преобразований процедуры криптографического преобразования.
2.6.35 этапный ключ: uz – босқич калити en – round key	Ключ этапа, формируемый на основе сеансово-этапного ключа.
2.7 Криптоанализ	
2.7.1 активная атака: uz – актив ҳужум en – active attack	1 Нападение путем внедрения в систему ложной информации или изменения существующей информации. 2 Реализация активной угрозы безопасности.

O'ZBEKISTON RESPUBLIKASI STANDARTLASHTIRISH, DAVLAT NAZORATINI MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARINI JORIY ETISH BOSHQARMASI

Термин		Определение
2.7.2	**активный нарушитель:** uz – актив бузғунчи (бузувчи) en – active intruder	Нарушитель, который пытается навязать ложные сообщения, перехватить и модифицировать сообщения, получить доступ к базам данных, расширить свои полномочия, навязать ложный открытый ключ, подготовить фиктивные документы, отказаться от подписи т.д.
2.7.3	**активная угроза:** uz – актив таҳдид en – active threat (danger)	Угроза намеренного несанкционированного изменения состояния системы.
2.7.4	**алгебраическая атака:** uz – алгебраик ҳужум en – algebraic attack	Метод криптоанализа, основанный на математических свойствах алгоритма шифрования.
2.7.5	**атака:** uz – ҳужум en – attack	1 Действие нарушителя, которое приводит к реализации угрозы путем использования уязвимостей автоматизированной системы. 2 Успешная или неудачная попытка взлома части или всей системы защиты информации.
2.7.6	**атака адаптивная:** uz – адаптив ҳужум en – adaptive attack	Атака на криптосистему, при которой характер воздействия противника и/или нарушителя может изменяться во времени в зависимости от действий законных пользователей криптосистемы или от других условий. Например, противник может подбирать различные исходные данные для воздействия на криптосистему.
2.7.7	**атака на криптосистему:** uz – криптотизимга қилинадиган ҳужум en – attack on the cryptosystem	Попытка противника и/или нарушителя понизить уровень безопасности конкретной криптографической системы на основе определенных методов криптоанализа и при некоторых предположениях криптоанализа.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT NAZORATINI MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARINI JORIY ETISH BOSHQARMASI

Термин	Определение
2.7.8 **атака по словарю:** uz – луғат бўйича ҳужум en – dictionary attack	Разновидность лобовой атаки, при которой перебираются пароли и/или подключается список заранее созданных паролей.
2.7.9 **атака перебором шифрованного текста:** uz – шифрланган матнни танлаш асосида ҳужум en – chosen cipher text attack	Метод криптоанализа, основанный на динамическом переборе зашифрованного текста, в условиях свободного доступа к части криптографического оборудования.
2.7.10 **атака грубой силы, полный перебор:** uz – қўпол куч ҳужуми, тўлиқ танлаш en – brute force attack	Атака, основанная на переборе всех или значительного количества возможных значений, пока не будет найдено верное.
2.7.11 **атака только по зашифрованному тексту:** uz – фақат шифрланган матн бўйича ҳужум en – cipher text only attack	Метод криптоанализа, основанный только на заданном шифротексте.
2.7.12 **бандитский криптоанализ:** uz – бандитларча криптотаҳлил en – brigandish cryptoanalysis	Частный случай атаки, для получения ключа «криптоаналитик» прибегает к угрозам, шантажу или пыткам. Возможно также взяточничество, которое иногда называют вскрытием с покупкой ключа.
2.7.13 **взлом, вскрытие криптосистемы:** uz – бузиш, криптотизимни очиш en – cracking (breaking), dissection of the cryptosystem	1 Создание процедуры, позволяющей вызывать отклонения информационного процесса, защищенного использованием криптосистемы, от условий его нормального протекания. 2 Нахождение способа решения задачи криптоанализа за разумное время при использовании современных вычислительных средств.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Термин		Определение
2.7.14	**дифференциальный криптоанализ:** uz – дифференциал криптотаҳлил en – differential cryptoanalysis	Метод криптоанализа симметричных блочных шифров (и других криптографических примитивов, в частности, хэш функций). Примечание - Основан на изучении преобразования разностей между шифруемыми значениями на различных раундах шифрования.
2.7.15	**компрометация:** uz – компрометация (обрўсизлантириш) en – compromising	Непреднамеренное раскрытие или обнаружение криптографического ключа или кода.
2.7.16	**криптоанализ:** uz – криптотаҳлил en – cryptoanalysis	1 Искусство и наука вскрытия шифра или объекта криптографии, любой другой формы. 2 Процесс получения исходного текста по шифрованному без знания ключа или процесс вычисления ключа по исходному и шифрованному тексту.
2.7.17	**линейный криптоанализ:** uz – чизиқли криптотаҳлил en - linear cryptanalysis	Метод криптоанализа, основанный на поиске линейной аппроксимации между исходным и шифрованным текстом.
2.7.18	**пассивный нарушитель:** uz – пассив бузғунчи (бузувчи) en – passive intruder	Нарушитель, не предпринимающий действий по дезорганизации криптографического протокола.
2.7.19	**пассивная угроза:** uz – пассив таҳдид en – passive threat	Угроза несанкционированного раскрытия информации без изменения состояния системы.
2.7.20	**противник:** uz – душман (рақиб) en – adversary	Субъект (специальная программа, оснащенная группа специалистов или физическое лицо), пытающийся преобразовать шифротекст в открытый текст без знания ключа или вычислить ключ по известным исходным и шифрованным текстам.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Термин	Определение
2.7.21 перебор открытого текста: uz – очиқ матнни танлаш en - adaptive-chosen-plaintext	Частный случай атаки методом перебора открытого текста, при котором криптоаналитик имеет возможность перебирать открытые тексты динамически и изменять их или алгоритм их перебора в зависимости от результатов предыдущих шифрований.
2.7.22 статистический криптоанализ: uz – статистик криптотаҳлил en - statistical cryptoanalysis	Вид криптоанализа, который исследует возможности взлома криптосистем на основе изучения статистических закономерностей исходных и зашифрованных сообщений.
2.7.23 частотный криптоанализ: uz – частотали криптотаҳлил en – frequency cryptoanalysis	Один из статистических методов раскрытия шифров, основанный на исследовании частоты появления знаков в криптограмме и сопоставлении ее с частотой появления знаков в исходном тексте.

2.8 Средства криптографической защиты информации (СКЗИ)

2.8.1 аппаратное средство защиты информации: uz – ахборотни муҳофаза қилишнинг аппарат воситаси en – hardware means of information protection	1 Специальное защитное устройство или приспособление, входящее в комплект технического средства обработки информации. 2 Механические, электромеханические, электронные, оптические, лазерные, радио, радиотехнические, радиолокационные и другие устройства, системы и сооружения, предназначенные для защиты информации от несанкционированного доступа, копирования, кражи или модификации.
2.8.2 аппаратный шифр: uz – аппарат шифри en – hardware cipher	Шифр, реализованный в виде средства вычислительной техники.

O'ZBEKISTON STANDARTLASHTIRISH, DAVLAT NAZORATINI MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARINI JORIY ETISH BOSHQARMASI

Термин		Определение
2.8.3	**аппаратно-программное средство защиты информации** uz – ахборотни муҳофаза қилишнинг аппарат-дастурий воситаси en – hardware - software means of information protection	Совокупность аппаратных и программных средств, входящих в состав информационно-коммуникационной системы, позволяющих обеспечить идентификацию и аутентификацию объектов, шифрование информации, управление криптографическими ключами, защиту от несанкционированного доступа, управление доступом и другие сервисы и механизмы информационной безопасности.
2.8.4	**безопасность эксплуатации СКЗИ:** uz – АКМҚВни эксплуатация қилиш хавфсизлиги en – exploitation security of CIPF	Совокупность мер управления и контроля, защищающая СКЗИ и криптографические ключи от несанкционированного (умышленного или случайного) их раскрытия, модификации, разрушения или использования.
2.8.5	**криптографический модуль:** uz – криптографик модуль en – cryptographic modul	Набор аппаратных, программных или аппаратно-программных компонентов, заключенных в пределах явно определенного, непрерывного периметра, реализующих утвержденные функции безопасности, включая криптографические алгоритмы, генерацию и распределение криптографических ключей, аутентификацию.
2.8.6	**криптографическое устройство:** uz – криптографик қурилма en – cryptographic device	Блок или узел электронной аппаратуры, реализующий криптографический алгоритм.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT NAZORATINI MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARINI JORIY ETISH BOSHQARMASI

Термин		Определение
2.8.7	**криптографическое оборудование:** uz – криптографик ускуна en – cryptographic equipment	1 Оборудование, в котором выполняются криптографические функции (например, шифрование, аутентификация, генерация ключей). 2 Аппаратные, программно-аппаратные, программные комплексы и средства для шифрования, расшифрования, хэширования, формирования и подтверждения подлинности ЭЦП, изготовления ключей и защиты от несанкционированного доступа, реализующие криптографические алгоритмы и предназначенные для защиты информации при ее передаче, обработке и хранении.
2.8.8	**программное средство защиты информации:** uz – ахборотни муҳофаза қилишнинг дастурий воситаси en – software means of information protection	Специальная программа, входящая в комплект программного обеспечения и предназначенная для защиты информации.
2.8.9	**роторная машина:** uz – ротор машина en – rotor machine	Механическое устройство шифрования, основанное на многоалфавитной подстановке, которая варьируется взаимным положением роторов.
2.8.10	**система криптографической защиты информации:** uz – ахборотни криптографик муҳофаза қилиш тизими en – cryptographic information protection system	Система, осуществляющая криптографическое преобразование информации для обеспечения ее безопасности.

O‘ZSTANDART AXBOROT MARKAZI
STANDARTLASHTIRISH, DAVLAT NAZORATINI MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARINI JORIY ETISH BOSHQARMASI

Термин		Определение
2.8.11	**СКЗИ:** uz – АКМҚВ en – CIPF	Аппаратное, программное или аппаратно-программное средство, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности.
2.8.12	**сертификация СКЗИ:** uz – АКМҚВни сертификатлаш en – certification of CIPF	Деятельность по подтверждению соответствия СКЗИ требованиям нормативно-правовых актов и государственных стандартов в установленном порядке.
2.8.13	**шифратор:** uz – шифрлагич, шифратор en – encoder, encipher	Электронное устройство или программа, реализующая алгоритмы шифрования.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

3 Алфавитный указатель терминов на русском языке

Абонентское шифрование 2.6.1
Авторизация 2.1.1
Администрация безопасности 2.1.2
Активная атака 2.7.1
Активный нарушитель 2.7.2
Активная угроза 2.7.3
Алгебраическая атака 2.7.4
Алгоритм 2.1.3
Алгебраическая степень нелинейности булевой функции 2.1.5
Алгоритм электронной цифровой подписи 2.4.3
Алгоритм ограниченного использования 2.1.4
Алгоритм аутентификации пользователя 2.4.1
Алгоритм шифрования данных 2.4.2
Алгоритм хэширования 2.4.4
Аппаратный шифр 2.8.2
Аппаратное средство защиты информации 2.8.1
Аппаратно-программное средство защиты информации 2.8.3
Асимметричный шифр 2.4.5
Асимметричное шифрование 2.4.6
Атака 2.7.5
Атака адаптивная 2.7.6
Атака на криптосистему 2.7.7
Атака по словарю 2.7.8
Атака перебором шифрованного текста 2.7.9
Атака только по зашифрованному тексту 2.7.11
Атака грубой силы, полный перебор 2.7.10
Аутентификация 2.1.6
Аутентификация пользователя 2.1.7
Аутентификация сообщения 2.1.8
Аутентичность 2.1.9
Аутентичный канал 2.1.10
Байт 2.1.11
Бандитский криптоанализ 2.7.12
Безопасность эксплуатации СКЗИ 2.8.4
Бесконфликтность 2.5.1
Бит 2.1.12
Биометрия 2.1.13
Биометрическая аутентификация 2.1.14
Биометрическая система 2.1.16
Биометрическая идентификация 2.1.15
Блок 2.1.17
Блочный алгоритм шифрования, блочный шифр 2.4.7
Вектор инициализации 2.1.18

O‘zSTANDART AGENTLIGI
STANDARTLASHTIRISH, O‘LCHASH
NAMATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Вероятностное шифрование 2.6.2
Владелец закрытого ключа ЭЦП 2.5.2
Владелец информации 2.1.19
Временный ключ 2.1.20
Взлом, вскрытие криптосистемы 2.7.13
Гамма шифра 2.1.21
Гаммирование 2.1.22
Генератор случайных чисел 2.1.23
Генератор псевдослучайных чисел 2.1.24
Генерация ключа 2.1.25
Генератор ключей 2.1.26
Группа 2.1.27
Гибкий шифр 2.6.3
Генератор ключей 2.1.26
Данные 2.1.29
Дайджест сообщения 2.1.28
Депонирование ключей 2.3.1
Дешифрование 2.6.4
Диаминор 2.6.6
Диапреобразование 2.6.7
Диаопределитель диаматрицы 2.6.8
Диаматрица 2.6.5
Дискретный логарифм 2.4.8
Дифференциальный криптоанализ 2.7.14
Дополнение 2.5.3
Допуск 2.1.32
Доступность информации 2.1.30
Достоверность информации 2.1.31
Закрытый ключ ЭЦП 2.5.4
Зашифрование данных 2.6.9
Защита информации 2.2.1
Защищаемая информация 2.2.2
Защита информации от утечки 2.2.3
Защита информации от несанкционированного воздействия 2.2.4
Защита информации от несанкционированного доступа 2.2.5
Защита информации от непреднамеренного воздействия 2.2.6
Защита информации от разглашения 2.2.7
Защита информации от разведки 2.2.8
Загрузчик ключа 2.1.33
Заявитель 2.1.34
Идентичность 2.1.35
Инициализирующее (начальное) значение 2.6.12
Информация 2.1.37
Информационная технология 2.1.38
Информационная система 2.1.39

O‘zSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI

Инфраструктура открытых ключей 2.5.5
Имитозащита 2.6.10
Имитовставка 2.6.11
Имитостойкость шифра 2.1.36
Канальное шифрование 2.6.13
Ключ обнаружения подделки ЭЦП 2.5.6
Ключ (криптографический) 2.3.12
Ключ шифрования 2.6.14
Ключ хэширования 2.5.7
Ключевой материал 2.3.14
Ключевое отношение 2.3.13
Коллизия 2.5.8
Коммутативность 2.4.9
Компонент ключа 2.3.15
Компрометация 2.7.15
Контрольный ключ 2.5.9
Конкатенация 2.4.10
Конфиденциальная информация 2.1.41
Конфиденциальность информации 2.1.42
Код аутентификации сообщения 2.1.40
Корреляционная иммунность булевой функции 2.1.43
Криптоаналитик 2.3.6
Криптоанализ 2.7.16
Криптография 2.3.4
Криптограф 2.3.5
Криптографическая защита 2.3.11
Криптографический модуль 2.8.5
Криптографический метод защиты информации 2.3.17
Криптографические примитивы 2.3.19
Криптографический протокол 2.3.7
Криптографическое преобразование 2.3.18
Криптографический алгоритм; алгоритм криптографического преобразования 2.4.11
Криптографическое оборудование 2.8.7
Криптографическая защита информации 2.3.10
Криптографическая синхронизация 2.3.20
Криптографическое устройство 2.8.6
Криптология 2.3.3
Криптопериод 2.3.16
Криптосистема эллиптической кривой (ECC) 2.4.12
Криптосистема с открытым ключом (асимметричная криптосистема) 2.3.9
Криптостойкость, криптографическая стойкость 2.3.8
Криптографическая система (криптосистема) 2.3.21
Лавинный эффект 2.1.44

O‘ZBEKISTON STANDARTLASHTIRISH, DAVLAT NAZORATINI MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARINI JORIY ETISH BOSHQARMASI

Линейный криптоанализ 2.7.17
Личные данные 2.1.45
Массив 2.1.46
Мероприятие по защите информации 2.2.9
Метод решета в числовом поле 2.4.13
Метод Полларда 2.4.14
Метод Полларда-Ро 2.4.15
Нелинейность булевой функции 2.1.48
Неотслеживаемость 2.1.47
Обновление ключей 2.3.2
Обратная диаматрица 2.6.15
Обратная матрица 2.6.16
Объект защиты информации 2.2.10
Однонаправленная функция 2.5.10
Орган защиты информации 2.2.11
Организация защиты информации 2.2.12
Открытый ключ ЭЦП 2.5.11
Отправитель электронного документа 2.5.12
Параметр алгоритма ЭЦП 2.5.13
Пассивный нарушитель 2.7.18
Пассивная угроза 2.7.19
Перебор открытого текста 2.7.21
Пластиковая карта 2.5.14
Перемешивание. 2.1.49
Перестановка. 2.1.50
Подстановочный шифр. 2.1.56
Подделка информации 2.1.51
Подтверждение подлинности ЭЦП 2.5.18
Подписанное сообщение 2.5.15
Поле Галуа 2.4.16
Пользователь информации (потребитель информации) 2.1.52
Пользователь открытого ключа ЭЦП 2.5.16
Полубайт 2.6.17
Получатель электронного документа 2.5.17
Показатель эффективности защиты информации 2.2.13
Последовательность случайных чисел 2.1.54
Последовательность псевдослучайных чисел 2.1.55
Помехоустойчивость шифра 2.1.53
Пороговая криптография: 2.1.57
Потоковый шифр 2.6.18
Предварительное распределение ключей. 2.1.58
Пространство ключей. 2.1.59
Проблема дискретного логарифма 2.4.17
Проблема дискретного логарифма на эллиптической кривой (ECDL) 2.4.18

O‘zSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Программное средство защиты информации 2.8.8
Протокол 2.1.60
Протокол рукопожатия..... 2.1.61
Псевдослучайная последовательность..... 2.1.62
Псевдослучайные числа..... 2.1.63
Противник 2.7.20
Процесс формирования ЭЦП и сеансового ключа 2.5.19
Процесс подтверждение подлинности ЭЦП 2.5.20
Разложение на множители методом эллиптической кривой 2.4.19
Расшифрование данных 2.6.19
Распределенный ключ 2.1.64
Расширение ключа 2.1.65
Раунд или цикл шифрования..... 2.6.20
Режимы шифрования..... 2.1.66
Режим шифрования со счетчиком 2.6.21
Режим электронной кодовой книги 2.1.67
Режим обратной связи по шифртексту 2.1.68
Режим обратной связи по выходу 2.1.69
Режим сцепление блоков шифротекста 2.2.14
Реквизиты электронного документа 2.5.21
Роторная машина 2.8.9
Свидетельство 2.5.22
Сеансовый ключ ЭЦП 2.5.23
Сеансово – этапный ключ 2.6.22
Секретный ключ 2.5.24
Сертификат ключа ЭЦП 2.5.25
Сертификат на средство ЭЦП 2.5.26
Сертификация СКЗИ..... 2.8.12
Совершенно нелинейная булевая функция (бент функция) 2.1.70
Согласование ключей..... 2.2.16
Составной шифр 2.2.17
Слепая подпись 2.5.27
Случайное число 2.1.72
Симметричный шифр 2.4.20
Симметричное шифрование 2.4.21
Симметричная криптосистема (криптосистема с секретным ключом) 2.3.22
Система защиты информации 2.2.15
Система криптографической защиты информации 2.8.10
Сообщение 2.1.71
Состояние 2.6.23
Способ защиты информации 2.2.18
Средство защиты информации 2.2.19
СКЗИ 2.8.11
Средства шифрования..... 2.6.24

STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Средства имитозащиты. 2.2.20
Средства ЭЦП 2.5.28
Средства кодирования 2.2.21
Срок безопасности 2.2.22
Стойкость криптолагоритма 2.2.23
Статический криптоанализ 2.7.22
Стеганография 2.3.23
Сцепление блоков 2.2.24
Теория чисел. 2.2.25
Традиционная криптография 2.2.26
Уничтожение информации 2.2.27
Управление ключами. 2.2.28
Уполномоченный орган. 2.2.29
Уравнение зашифрования 2.2.30
Уравнение расшифрования 2.2.31
Участник электронной коммерции 2.5.29
Факторизация 2.4.22
Фактор 2.4.23
Функция криптографическая 2.6.25
Функция сжатия 2.5.30
Функция шифрования 2.6.26
Функциональный ключ 2.6.27
Функция – ловушка 2.2.32
Хранение ключа. 2.2.33
Хэширование 2.5.33
Хэш-код 2.5.32
Хэш-функция (функция хэширования) 2.5.34
Хэш, хэш-значение 2.5.31
Цель защиты информации 2.2.34
Центр доверия 2.2.35
Центр регистрации ключей ЭЦП 2.5.35
Центр распределения ключей. 2.2.36
Цикл жизненный ключей 2.2.37
Цифровой отпечаток 2.2.38
Шифрование информации 2.6.33
Шифр 2.6.29
Шифр совершенный 2.6.30
Шифрование с открытым ключом 2.6.32
Шифратор 2.8.13
Шифрование сеанса 2.6.28
Шифртекст, зашифрованный текст 2.6.31
Частотный криптоанализ 2.7.23
Экспорт шифрования 2.2.39
Экспоненциальное время. 2.3.25
Энтропия. 2.3.24

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Электронные деньги 2.5.39
Электронная коммерция 2.5.40
Электронный документ 2.5.37
Электронный документооборот 2.5.38
Эллиптическая кривая 2.4.24
Электронный платёж 2.5.41
Электронная цифровая подпись, ЭЦП 2.5.36
Эффективность защиты информации 2.2.40
Этап 2.6.34
Этапный ключ 2.6.35
Этапный ключ хэширования 2.5.42
Ячейка 2.1.73

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

4 Алфавитный указатель терминов на узбекском языке

Абонент шифрлаши 2.6.1
Авторизация қилиш 2.1.1
Адаптив ҳужум 2.7.6
Айнан ўхшашлик 2.1.35
Алгебраик ҳужум 2.7.4
Алгоритм 2.1.3
Актив ҳужум 2.7.1
Актив бузғунчи (бузувчи) 2.7.2
Актив таҳдид 2.7.3
Анъанавий криптография. 2.2.26
Аппарат шифри 2.8.2
Асимметрик шифр 2.4.5
Асимметрик шифрлаш 2.4.6
Ахборот 2.1.37
Ахборот эгаси 2.1.19
Ахборотдан фойдалана олишлик 2.1.30
Ахборотнинг ишончлилиги 2.1.31
Ахборотни йўқ қилиш 2.2.27
Ахборотни чиқиб кетишдан муҳофаза қилиш 2.2.3
Ахборотни рухсат этилмаган таъсирдан муҳофаза қилиш 2.2.4
Ахборотни рухсатсиз фойдаланишдан муҳофаза қилиш 2.2.5
Ахборотни қасддан қилинмаган ҳаракатдан муҳофаза қилиш 2.2.6
Ахборотни ошкор этилишдан муҳофаза қилиш 2.2.7
Ахборотни разведкадан муҳофаза қилиш 2.2.8
Ахборотни муҳофаза қилиш 2.2.1
Ахборотни муҳофаза қилиш тадбири 2.2.9
Ахборотни муҳофаза қилиш объекти 2.2.10
Ахборотни сохталаштириш 2.1.51
Ахборот технологияси 2.1.38
Ахборот тизими 2.1.39
Ахборот муҳофаза қилишни ташкил этиш. 2.2.12
Ахборотни муҳофаза қилиш органи 2.2.11
Ахборот фойдаланувчиси (ахборот истеъмолчиси) 2.1.52
Ахборотни муҳофаза қилиш самарадорлиги 2.2.40
Ахборотни муҳофаза қилиш самарадорлигининг кўрсаткичи 2.2.13
Ахборотни муҳофаза қилиш тизими 2.2.15
Ахборотни криптографик муҳофаза қилиш тизими 2.8.10
Ахборотнинг криптографик муҳофаза қилиш. 2.3.10
АКМҚВ 2.8.11
АКМҚВни сертификатлаш 2.8.12
АКМҚВ экслуатация қилиш хавфсизлиги 2.8.4
Ахборот муҳофаза қилиш мақсади 2.2.34
Ахборотни муҳофаза қилиш усули 2.2.18

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT NAZORATINI MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARINI JORIY ETISH BOSHQARMASI

Ахборотни муҳофаза қилиш воситаси 2.2.19
Ахборотни муҳофаза қилишнинг аппарат воситаси 2.8.1
Ахборотни муҳофаза қилишнинг дастурий воситаси 2.8.7
Ахборотни муҳофаза қилишнинг аппарат-дастурий воситаси 2.8.3
Ахборотни муҳофаза қилишнинг криптографик усули 2.3.17
Ахборотни шифрлаш 2.6.33
Ахборотнинг конфиденциаллиги 2.1.42
Аутентификация қилиш (ҳақиқийликни тасдиқлаш) 2.1.6
Ҳақиқий канал. 2.1.10
Аралаштириш 2.1.49
Бандитларча криптотаҳлил 2.7.12
Байт 2.1.11
Бир томонлама функция 2.5.10
Биометрия 2.1.13
Биометрик тизим 2.1.16
Биометрик аутентификация қилиш. 2.1.14
Биометрик идентификация қилиш. 2.1.15
Бит 2.1.12
Блок 2.1.17
Блокли шифрлаш алгоритми, блокли шифр 2.4.7
Блокларни боғлаш 2.2.24
Босқич 2.6. 34
Босқич калити 2.6. 35
Буль функциясининг алгебраик чизиқсизлик даражаси 2.1.5
Буль функциясининг корреляцион бардошлилиги 2.1.43
Буль функция чизиқсизлилиги 2.1.48
Бузиш, криптотизимни очиш 2.7.13
Бўсағавий криптография 2.1.57
Ваколатли орган 2.2.29
Вақтинчалик калит. 2.1.20
Гаммалаш 2.1.22
Галуа майдони 2.4.16
Гувоҳнома 2.5.22
Группа. 2.1.27
Дастлабки матнга ўгириш тенгламаси 2.2.31
Даъво қилувчи 2.1.34
Диаминор 2.6.6
Диаалмаштириш 2.6.7
Диаматрица диааниқловчиси 2.6.8
Диаматрица 2.6.5
Дискрет логарифм 2.4.8
Дискрет логарифм муаммоси 2.4.17
Дифференциал криптотаҳлил 2.7.14
Душман (рақиб). 2.7.20
Кўчки (лавина) эффекти. 2.1.44

O‘ZBEKISTON RESPUBLIKASI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Зиддиятсизлик 2.5.1
Зичлаш функцияси 2.5.30
Имзоланган хабар 2.5.15
Имитомуҳофаза 2.6.10
Имитомуҳофаза воситалари 2.2.20
Имитоқўшимча 2.6.11
Инициализация вектори. 2.1.18
Инициализацияловчи (бошланғич) қиймат 2.6.12
Ишонч маркази 2.2.35
Калитлар генератори 2.1.26
Каналли шифрлаш 2.6.13
Калит (криптографик) 2.3.12
Калит генерацияси. 2.1.25
Калитлар генератори 2.1.26
Калит юкловчи 2.1.33
Калит компоненти 2.3.15
Калитларни олдиндан тақсимлаш. 2.1.58
Калитлар майдони 2.1.59
Калитларни бошқариш 2.2.28
Калитни кенгайтириш 2.1.65
Калитларни мувофиқлаштириш.. . . . . 2.2.16
Калитни сақлаш 2.2.33
Калитларни сақлаш учун топшириш 2.3.1
Калитларни тақсимлаш маркази. 2.2.36
Калитларни янгилаш 2.3.2
Калитларнинг ҳаётий цикли 2.2.37
Калитли маълумот 2.3.14
Калитли муносабат 2.3.13
Кодлаш воситалари 2.2.21
Коллизия 2.5.8
Коммутативлик 2.4.9
Компрометация (обрўсизлантириш) 2.7.15
Конкатенация 2.4.10
Криптодавр 2.3.16
Криптология 2.3.3
Криптография 2.3.4
Криптограф 2.3.5
Крипотаҳлилчи 2.3.6
Крипотаҳлил 2.7.16
Криптографик тизим (криптотизим) 2.3.21
Криптографик протокол 2.3.7
Криптоалгаритмнинг бардошлилиги 2.2.23
Криптобардошлилик, криптографик бардошлилик 2.3.8
Криптографик алгоритм, криптографик алмаштириш алгоритми 2.4.11
Криптографик алмаштириш 2.3.18

O'ZBEKISTON AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Криптографик ускуна 2.8.7
Криптографик муҳофаза қилиш 2.3.11
Криптографик примитивлар 2.3.19
Криптографик синхронизация 2.3.20
Криптографик қурилма 2.8.6
Криптографик модуль 2.8.5
Криптографик функция 2.6.25
Криптотизимга қилинадиган ҳужум 2.7.7
Кўр-кўрона имзо 2.5.27
Массив 2.1.46
Махфий калит 2.5.24
Маълумотлар 2.1.29
Маълумотларни шифрматнга ўгириш 2.6.9
Маълумотларни дастлабки матнга ўгириш 2.6.19
Муҳофаза қилинадиган ахборот 2.2.2
Маълумотларни шифрлаш алгоритми 2.4.2
Мослашувчан шифр 2.6.3
Мутлақо чизиқсиз буль функцияси (бент функция) 2.1.70
Луғат бўйича ҳужум 2.7.8
Назорат калити 2.5.9
Очиқ калитлар инфратузилмаси 2.5.5
Очиқ калитли шифрлаш 2.6.32
Очиқ калитли криптотизим (асимметрик криптотизим) 2.3.9
Очиқ матнни танлаш 2.7.21
Пассив бузғунчи (бузувчи) 2.7.18
Пассив таҳдид 2.7.19
Пластик карта 2.5.14
Конфиденциал ахборот 2.1.41
Псевдотасодифий сонлар 2.1.63
Псевдотасодифий сонлар кетма-кетлиги 2.1.55
Псевдотасодифий сонлар генератори. 2.1.24
Псевдотасодифий кетма-кетлик 2.1.62
Полларда усули 2.4.14
Полларда – Ро усули 2.4.15
Протокол (баённома) 2.1.60
Рақамли из 2.2.38
Ротор машина 2.8.9
Сеанс калити 2.5.23
Сеанс – босқич калити 2.6.22
Симметрик шифр 2.4.20
Симметрик криптотизим (махфий калитли криптотизим) 2.3.22
Сонли майдонда панжара усули 2.4.13
Сонлар назарияси. 2.2.25
Статистик криптотаҳлил 2.7.22
Стеганография 2.3.23

STANDARTLASHTIRISH, DAVLAT
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Такомиллашган шифр 2.6.30
Таъқиб эта олмаслик 2.1.47
Тақсимланган калит. 2.1.64
Тасодифий сон 2.1.72
Тасодифий сонлар кетма-кетлиги 2.1.54
Тасодифий сонлар генератори. 2.1.23
Тескари диаматрица 2.6.15
Тескари матрица 2.6.16
Туб кўпайтувчиларга ажратиш (факторлаштириш) 2.4.22
Эллиптик эгри чизиқ усулида туб кўпайтувчиларга ажратиш 2.4.19
Тузоқ функция. 2.2.32
Тўлдирувчи 2.5.3
Оқимли (узлуксиз шифр) 2.6.18
Фактор 2.4.23
Фақат шифрланган матн бўйича ҳужум 2.7.11
Фойдаланувчини аутентификация қилиш 2.1.7
Фойдаланувчини аутентификация қилиш алгоритми 2.4.1
Фойдаланиши чекланган алгоритм 2.1.4
Фойдаланиш ҳуқуқи. 2.1.32
Функционал калит 2.6.27
Хавфсизлик маъмурияти 2.1.2
Хавфсизлик муддати 2.2.22
Хабар 2.1.71
Хабарни аутентификация қилиш 2.1.8
Хабар дайжести 2.1.28
Хабарни аутентификация қилиш коди 2.1.40
Хэшлаш 2.5.33
Хэш-код 2.5.32
Хэш-функция (хэшлаш функцияси) 2.5.34
Хэш, хэш-қиймат 2.5.31
Хэшлаш алгоритми 2.4.4
Хэшлаш калити 2.5.7
Хэшлашнинг босқич калити 2.5.42
Частотали криптотаҳлил 2.7.23
Чизиқли криптотаҳлил 2.7.17
Чиқиш қийматлари бўйича тескари алоқа режими 2.1.69
Шахсий маълумотлар 2.1.45
Шифрлаш калити 2.6.14
Шифрлаш функцияси 2.6.26
Шифрлаш раунди ёки цикли 2.6.20
Шифрлагич, шифратор 2.8.13
Шифр 2.6.29
Шифр матн, шифрланган матн 2.6.31
Шифр матн блоклари боғланиши 2.2.14
Шифр матн бўйича тескари алоқа режими 2.1.68

O'ZBEKISTON AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Шифрланган матнни танлаш асосида ҳужум 2.7.9
Шифрни калитсиз очиш (дешифрлаш) 2.6.4
Шифр гаммаси 2.1.21
Шифрнинг имитобардошлилиги 2.1.36
Шифрлаш режимлари 2.1.66
Шифрлаш воситалари 2.6.24
Шифрлаш сеанси 2.6.28
Шифрлаш тенгламаси 2.2.30
Шифрлаш функцияси 2.6.26
Шифрлаш экспорти 2.2.39
Шифрнинг халақит бардошлилиги 2.1.53
Эҳтимолий шифрлаш 2.6.2
Экспоненциал вақт. 2.3.25
Электрон код китоби режими 2.1.67
ЭРИ ёпиқ калитининг эгаси 2.5.2
Электрон тижорат 2.5.40
Электрон пуллар 2.5.39
Электрон ҳужжат 2.5.37
Электрон ҳужжатни жўнатувчи 2.5.12
Электрон ҳужжат айланиши 2.5.38
Электрон ҳужжат реквизитлари 2.5.21
Электрон тижорат иштирокчиси 2.5.30
Электрон тўлов 2.5.41
Электрон рақамли имзо, ЭРИ 2.5.36
ЭРИ воситалари 2.5.28
Электрон рақамли имзо алгоритми 2.4.3
Электрон ҳужжатни қабул қилиб олувчи 2.5.17
ЭРИнинг ҳақиқийлигини тасдиқлаш 2.5.18
ЭРИнинг сохталаштирилганлигини аниқлаш жараёни 2.5.19
ЭРИнинг ҳақиқийлигини тасдиқлаш жараёни 2.5.20
ЭРИ очиқ калити фойдаланувчиси 2.5.16
ЭРИ алгоритмининг параметри 2.5.13
ЭРИнинг ёпиқ калити 2.5.4
ЭРИнинг очиқ калити 2.5.11
ЭРИни сохталаштирилганлигини аниқлаш калити 2.5.6
ЭРИ калитларини рўйхатга олиш маркази 2.5.35
ЭРИ калити сертификати 2.5.25
ЭРИ воситасига сертификат 2.5.26
Эллиптик эгри чизиқ 2.4.24
Эллиптик эгри чизиқли криптотизим 2.4.12
Эллиптик эгри чизиқли дискрет логарифм муаммоси 2.4.18
Энтропия. 2.3.24
Яримбайт 2.6.17
Ячейка 2.1.73
Ўрин алмаштириш 2.1.50

O‘ZBEKISTON RESPUBLIKASI DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Ўрнига қўйиш шифри 2.1.56
Қўл сиқишув протоколи. 2.1.61
Қўшма (таркибли) шифр 2.2.17
Қўпол куч ҳужуми, тўлиқ танлаш 2.7.10
Ҳақиқийлик 2.1.9
Ҳақиқий канал 2.1.10
Ҳисоблагич бўйича шифрлаш режими 2.6.21
Ҳолат 2.6.23
Ҳужум 2.7.5

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

5 Алфавитный указатель терминов на английском языке

Adversary 2.7.20
Adaptive-chosen-plaintext 2.7.21
Appendix 2.5.3
Absolutely nonlinear Boolean function (bent function) 2.1.70
Active attack 2.7.1
Active intruder 2.7.2
Active threat (danger) 2.7.3
Adaptive attack 2.7.6
Algebraic attack 2.7.4
Algebraic degree of nonlinearity of Boolean function 2.1.5
Algorithm 2.1.3
Asymmetric cipher 2.4.5
Asymmetric encryption 2.4.6
Authentication 2.1.6
Authorization 2.1.1
Authenticity 2.1.9
Authority of information protection 2.2.11
Authentication of EDS 2.5.18
Attack 2.7.5
Attack on the cryptosystem 2.7.7
Avalanche effect 2.1.44
Byte 2.1.11
Bit 2.1.12
Biometrics 2.1.13
Biometric(al) system 2.1.16
Biometric authentication 2.1.14
Biometric identification 2.1.15
Blind signature 2.5.27
Block 2.1.17
Block chaining 2.2.24
Block ciphering algorithm, block cipher 2.4.7
Brute force attack 2.7.10
Brigandish cryptoanalysis 2.7.12
Cell 2.1.73
Center of EDS keys registration 2.5.35
Certificate for public key EDS 2.5.25
Certificate for EDS means 2.5.26
Certification of CIPF 2.8.12
Chosen cipher text attack 2.7.9
Channel encryption 2.6.13
Cipher 2.6.29
Cipher Block Chaining 2.2.14
Ciphering function 2.2.30

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Cipher feed back (CFB) mode 2.1.68
Cipher text only attack 2.7.11
Ciphertext, enciphered text 2.6.31
Collision-free 2.5.1
Collision 2.5.8
Coding tools 2.2.21
Compound cipher 2.2.17
Commutativety 2.4.9
Confidentiality of information 2.1.42
Compromising 2.7.15
Compression function 2.5.30
Concatenation 2.4.10
Control key 2.5.9
Correlational immunity of Boolean function 2.1.43
Counter (CTR) mode 2.6.21
Cracking (breaking), dissection of the cryptosystem 2.7.13
Cryptology 2.3.3
Cryptography 2.3.4
Cryptographer 2.3.5
Cryptanalyst 2.3.6
Cryptoanalysis 2.7.16
Cryptographic system (cryptosystem) 2.3.21
Cryptographic algorithm 2.4.11
Cryptographic function 2.6.25
Cryptographic modul 2.8.5
Cryptographic equipment 2.8.7
Cryptographic protocol 2.3.7
Cryptographic strength 2.3.8
Cryptosystem with public key 2.3.9
Cryptographic transformation 2.3.18
Cryptographic primitives 2.3.19
Cryptographic protection 2.3.11
Cryptographic device 2.8.6
Cryptographic information protection system 2.8.10
Cryptographic method of information protection 2.3.17
CIPF 2.8.11
Cryptographic protection to information 2.3.10
Cryptographic synchronization 2.3.20
Cryptoperiod 2.3.16
Data 2.1.29
Data falsification 2.1.51
Data encryption algorithm 2.4.2
Deciphering data 2.6.19
Deciphering function 2.2.31
Declarant 2.1.34

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT NAZORATINI MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARINI JORIY ETISH BOSHQARMASI

Decryption 2.6.4
Diaminor 2.6.6
Diadeterminant of the diamatrix 2.6.8
Diatransformation 2.6.7
Diamatrix 2.6.5
Digital timestamp 2.6.11
Digital imprint 2.2.38
Differential cryptanalysis 2.7.14
Discrete logarithm 2.4.8
Ddistributed key 2.1.54
Dictionary attack 2.7.8
Discrete logarithm problem 2.4.17
Efficiency of information Protection 2.2.40
Efficiency of information protection indicator 2.2.13
Electronic code book (ECB) mode 2.1.67
Electronic documents attributes 2.5.21
Electronic commerce 2.5.40
Electronic money, e-money 2.5.39
Electronic document 2.5.37
Electronic documents circulation 2.5.38
Electronic payment 2.5.41
Electronic digital signature, EDS 2.5.36
Electronic digital signature algorithm 2.4.3
Encryption function 2.6.26
Enciphering data 2.6.9
Encryption key 2.6.14
Entropy 2.3.24
Elliptic curve 2.4.24
Elliptic curve (factoring) method 2.4.19
Elliptic curve cryptosystem 2.4.12
Elliptic curve discrete logarithm (ECDL) problem 2.4.18
Encoder, encipher 2.8.13
Export of cryptooperation 2.2.39
Exponential time 2.3.25
Exploitation security of CIPF. 2.8.4
Falsification detection key EDS 2.5.6
Falsification detection process EDS 2.5.19
Factoring 2.4.22
Facilities of the cryptooperation 2.6.24
Facilities electronic EDS 2.5.28
Field (spase) of keys 2.1.59
Factor 2.4.23
Flexible cipher 2.6.3
Functional key 2.6.27
Function-trap 2.2.32

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Frequency cryptoanalysis 2.7.23
Galois field 2.4.16
Gamma of the cipher 2.1.21
Gamma 2.1.22
Group 2.1.27
Key agreement 2.2.16
Key generation 2.1.25
Key generator. 2.1.26
Key loader. 2.1.33
Key lifetime. 2.2.37
Key material. 2.3.14
Key escrow. 2.3.13
Key extention. 2.1.65
Key distribution centre. 2.2.36
Key (cryptographic) 2.3.12
Key component. 2.3.15
Key relations. 2.3.13
Key updating. 2.3.2
Keeping of the key. 2.2.33
Handshake protocol. 2.1.61
Hardware cipher. 2.8.2
Hardware means of information protection 2.8.1
Hardware - software means of information protection 2.8.3
Hashing 2.5.33
Hashing algorithm. 2.4.4
Hash-code. 2.5.32
Hash-function. 2.5.34
Hashing key. 2.5.7
Hashing round key 2.5.42
Hash, hash-value. 2.5.31
Identity. 2.1.35
Information owner. 2.1.19
Information availability 2.1.30
Information validity 2.1.31
Information protection 2.2.1
Information protection from leak. 2.2.3
Information protection from unauthorized action. 2.2.6
Information protection from unauthorized access 2.2.5
Information protection from inadvertent action 2.2.4
Information protection from disclosure 2.2.7
Information protection from exploration 2.2.8
Information 2.1.37
Information destruction. 2.2.27
Information encryption. 2.6.33
Information user (consumer) 2.1.52

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Information protection object 2.2.10
Information protection development. 2.2.12
Information protection system 2.2.15
Information protection method 2.2.18
Information protection tools 2.2.19
Information technology 2.1.38
Information system 2.1.39
Iinitialization vector. 2.1.18
Initial key distribution. 2.1.58
Initial value. 2.6.12
Imitational protection. 2.6.10
Imitoresistance of cipher. 2.1.36
Imitoprotection means. 2.2.20
Key management. 2.2.28
Linear cryptoanalysis. 2.7.17
Limited use algorithm 2.1.4
Massive. 2.1.46
Measure protection of information. 2.2.9
Message. 2.1.71
Message digest. 2.1.28
Message authentication. 2.1.8
Message authentication code. 2.1.40
Modes of the cryptooperation. 2.1.66
Mixing 2.1.49
Number field sieve. 2.4.13
Number theory. 2.2.25
Nibble (half byte) 2.6.17
Noise stability of a cipher. 2.1.53
Nonlinearity of Boolean function. 2.1.48
One-way function. 2.5.10
Owner of private key of the EDS 2.5.2
Output feed back (OFB) mode. 2.1.69
Parameter of algorithm of EDS. 2.5.13
Passive threat (danger) 2.7.19
Passive intruder. 2.7.18
Permutation. 2.1.50
Plastic card 2.5.14
Participants of electronic commerce. 2.5.29
Perfect cipher 2.6.30
Period or cycle of ciphering 2.6.20
Personal data 2.1.45
Pollard method 2.4.14
Pollard Rho method 2.4.15
Public key user EDS 2.5.16
Phase-session key 2.6.22

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Public key infrastructure, PKI 2.5.5
Purpose of information protection 2.2.34
Public key encryption 2.6.32
Private key of EDS 2.5.11
Protocol 2.1.60
Protected information 2.2.2
Private key 2.5.24
Probabilistic encryption 2.6.2
Pseudo-random number sequence 2.1.55
Pseudorandom sequence 2.1.62
Pseudorandom number generator 2.1.24
Pseudorandom numbers 2.1.63
Random number 2.1.72
Random number generator 2.1.23
Random number sequence 2.1.54
Reverse diamatrix 2.6.15
Reverse matrix 2.6.16
Receiver of electronic document 2.5.17
Representative authority 2.2.29
Rotor machine 2.8.8
Round 2.6.34
Round key 2.6.35
Sender of the electronic document 2.5.12
Security administrator 2.1.2
Security period 2.2.22
Session key 2.5.23
Session encryption 2.6.28
Sensitive (confidential) information 2.1.41
Signed message 2.5.15
Software means of information protection 2.8.7
Subscriber encryption 2.6.7
Substitution cipher 2.1.56
Stability of cryptoalgorithm 2.2.23
State 2.6.23
Stream cipher 2.6.18
Statistical cryptoanalysis 2.7.22
Steganography 2.3.23
Symmetric cryptosystem, (cryptosystem with private key) 2.3.22
Symmetric cipher 2.4.20
Symmetric encryption 2.4.21
Temporary key 2.1.20
The authentic channel 2.1.10
Tolerance 2.1.32
Threshold cryptography 2.1.57
Traditional cryptography 2.2.26

O'zDSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Trusted centre 2.2.35
User autentification 2.1.7
User autentification algorithm 2.4.1
Untracebility 2.1.47
Verification processes EDS 2.5.20
Witness 2.5.22

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

УДК 621.391 ОКС 01.040.35 Группа П 85

Ключевые слова: алгоритм шифрования данных, шифротекст, зашифрование данных, расшифрование данных, криптология, криптография, криптографическая защита информации, криптоанализ

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

O‘z DSt 1109:2013

В.и.о. директора
ГУП «UNICON.UZ» Х.Хасанов

Начальник научно-
исследовательского
отдела криптографии О.Ахмедова

Младший научный сотрудник Д.Джаматова

Нормоконтроль Л.Шаймарданова

СОГЛАСОВАНО

Заместитель начальника отдела
информационной безопасности
Государственного комитета связи,
информатизации и информационных
технологий Республики Узбекистан

А.Гафуров
письмо от 17.04.2013
№ 14-8/1876

СОГЛАСОВАНО

Заместитель Председателя СНБ

А.А. Курбанов
письмо от 05.06.2013
№ 39/1939

СОГЛАСОВАНО

Начальник Государственной
инспекции по надзору в сфере связи,
информатизации и
телекоммуникационных технологий

Ф.Умарходжаев
письмо от 25.02.2013
№ 32-13/283