O‘z DSt _____ :2015

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ УЗБЕКИСТАН

Информационная технология

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Термины и определения

Издание официальное

Узбекское агентство стандартизации, метрологии и сертификации

Ташкент

O‘z DSt 1927:2015

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 телекоммуникационных технологий № 7

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ постановлением Узбекского агентства стандартизации, метрологии и сертификации (агентство «Узстандарт») от 05.02.2015 № 05-619

4 ВЗАМЕН O‘z DSt ISO/IEC 2382-8:2007 и TSt 45-010:2010

Информация о введении в действие (прекращении действия) настоящего стандарта и изменений к нему на территории Республики Узбекистан 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»

Содержание

1 Область применения 1
2 Термины и определения 1
2.1 Основные понятия 1
2.2 Характеристики безопасности информации 5
2.3 Требования по безопасности информации 6
2.4 Управление информационной безопасностью 8
2.5 Безопасность информации 9
2.6 Угрозы информационной безопасности 11
2.7 Риски 20
2.8 Атаки 22
2.9 Управление доступом 24
2.10 Методы защиты информации 32
2.11 Криптографические методы защиты информации 34
2.12 Защита чувствительной информации 36
2.13 Средства защиты информации 41
2.14 Информационная безопасность сетей телекоммуникаций . 45
2.15 Информационная безопасность мобильной связи 53
2.16 Режим секретности 54
2.17 Защита и восстановление данных 59
2.18 Защита от копирования 61
3 Алфавитный указатель терминов на русском языке 63
4 Алфавитный указатель терминов на узбекском языке 75
5 Алфавитный указатель терминов на английском языке 87

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, AKTLAT
MAZMUNI MUVOFIQLIGINI TASDIQLASH
AKSIDAN TEKSH
JORIY ETISH

Введение

Установленные в настоящем стандарте термины расположены в систематизированном порядке, отражающем систему понятий в данной области знаний.

Для каждого понятия установлен один стандартизованный термин.

Заключенная в круглые скобки часть термина может быть опущена при использовании термина в документах по стандартизации. При этом не входящая в круглые скобки часть термина образует его краткую форму.

Наличие квадратных скобок в терминологической статье означает, что в нее включены два термина, имеющие общие терминоэлементы.

Для удобства пользования стандартом приведены алфавитные указатели терминов на русском (ru), узбекском (uz) и английском (en) языках с указанием соответствующих номеров терминологических статей.

Стандартизованные термины набраны полужирным шрифтом, их краткие формы, представленные аббревиатурой, – светлым, а синонимы - курсивом.

В настоящем стандарте использованы следующие сокращения:

CDMA2000 (Code Division Multiple Access)	стандарт мобильной связи третьего поколения с кодовым методом доступа абонентов в сеть
GSM (Global System for Mobile Communications)	глобальный стандарт цифровой мобильной связи с разделением каналов по времени и частоте
UMTS (Universal Mobile Telecommunications System)	стандарт мобильной связи третьего поколения, обеспечивающий предоставление широкополосного доступа с кодовым разделениям каналов

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH INSTITUTI
MAZORAT...
AXBOROT TEXNO...
JORIY ETISH...

O‘z DSt 2927 :2015

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ УЗБЕКИСТАН

Ахборот технологияси

АХБОРОТ ХАВФСИЗЛИГИ

Атамалар ва таърифлар

Информационная технология

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Термины и определения

Information technology

Information security

Terms and definitions

Дата введения 09.02.2015

1 Область применения

Настоящий стандарт устанавливает основные термины и их определения в области безопасности информационных технологий.

Стандарт предназначен для облегчения общения специалистов в области информационной безопасности и информационных технологий.

Установленные термины обязательны для применения во всех видах документации.

2 Термины и определения

2.1 Основные понятия

2.1.1 **административная безопасность;** *процедурная безопасность*: Административные меры, направленные на обеспечение компьютерной безопасности.

Примечание – К этим мерам относятся операционные процедуры и процедуры подотчетности, процедуры расследования нарушений безопасности и анализ журналов аудита.

uz – маъмурий хавфсизлик, процедура хавфсизлиги

en – administrative security, procedural security

Издание официальное

O'ZSTANDART AGENTLIGI
5449 son bilan
«05» 02 2015 yildа
Davlat ro'yxatiga olindi

2.1.2 **безопасность:** Способность объекта противостоять воздействиям случайных и преднамеренных угроз.

uz – хавфсизлик
en – security

2.1.3 **доверенная компьютерная система:** Система обработки данных, в которой предусмотрена достаточная компьютерная безопасность с учетом возможности одновременного доступа пользователей к данным с разными грифами секретности и категориями безопасности.

uz – ишончли компьютер тизими
en – trusted computer system

2.1.4 **защищенное средство вычислительной техники [защищенная автоматизированная система]:** Средство вычислительной техники (автоматизированная система), в котором реализован комплекс средств защиты.

uz – ҳисоблаш техникасининг муҳофаза қилинган воситаси [муҳофаза қилинган автоматлаштирилган тизим]
en – protected facility of computing machinery [protected computer-based system]

2.1.5 **защищенное техническое средство информатизации:** Техническое средство информатизации, в котором реализован комплекс средств защиты от нарушения целостности и утечки по техническим каналам обрабатываемой на них информации.

uz – ахборотлаштиришни муҳофаза қилинган техник воситаси
en – protected technical facility of informatization

2.1.6 **злоумышленник;** *нарушитель*: Лицо или организация, заинтересованные в получении несанкционированного доступа к информационной системе и ее ресурсам и совершившие преднамеренные действия для их несанкционированного получения или изменения.

uz – жиноятқор, бузувчи
en – intruder, hacker, violator

2.1.7 **информационная безопасность:** Защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений.

uz – ахборот хавфсизлиги
en – information security

2.1.8 **инцидент:** Любое событие, которое приводит или может привести к незапланированному прерыванию услуги или к снижению ее качества.

Примечание - Примером инцидента является сбой в одном из элементов инфраструктуры.

uz – инцидент
en – incident

2.1.9 **инцидент информационной безопасности:** Единичное событие или ряд нежелательных или непредвиденных событий информационной безопасности, из-за которых велика вероятность компрометации защищаемой информации и реализации угрозы информационной безопасности.

uz – ахборот хавфсизлиги инциденти
en – incident of information security

2.1.10 **коммуникационная безопасность;** *безопасность связи*: Компьютерная безопасность применительно к передаче данных.

uz – коммуникацион хавфсизлик, алоқа хавфсизлиги
en – communications security

2.1.11 **компьютерная безопасность:** Защита данных и ресурсов от случайных или злоумышленных несанкционированных действий, обычно путем проведения соответствующих мероприятий.

Примечание – К этим несанкционированным действиям относятся модификация, уничтожение, доступ, раскрытие или сбор данных.

uz – компьютер хавфсизлиги
en – computer security

2.1.12 **логический объект:** Любая именованная составляющая компьютерной системы, которая может быть представлена в терминах некоторого языка.

Примечание - Логические объекты подразделяются на объекты и субъекты.

uz – мантиқий объект
en – entity

2.1.13 **обработка информации:** Совокупность операций сбора, накопления, ввода, вывода, приема, передачи, записи, хранения, регистрации, уничтожения, преобразования, отображения информации.

uz – ахборотни қайта ишлаш
en – information processing

2.1.14 **объект:** Логический объект, доступ к которому контролируется.

Примечание – Логическим объектом может быть файл, программа, область оперативной памяти, собранные и хранимые персональные данные.

uz – объект
en – object

O‘ZSTANDART AGENTLIGI

2.1.15 **объект информатизации:** Информационные системы различного уровня и назначения, сети телекоммуникаций, технические средства обработки информации, помещения, где установлены и эксплуатируются эти средства, а также помещения, предназначенные для ведения переговоров, в т.ч. конфиденциальных.

uz – ахборотлаштириш объекти
en – object of informatization

2.1.16 **остаточная информация:** Информация на запоминающем устройстве, оставшаяся от формально удалённых операционной системой данных или из-за физических свойств запоминающих устройств.

uz – қолдиқ ахборот
en – residual information

2.1.17 **пользователь [потребитель] информации:** Субъект, обращающийся к информационным ресурсам за получением необходимой ему информации и пользующийся ею.

uz – ахборот фойдаланувчи [ахборот истеъмолчиси]
en – information user

2.1.18 **приватность:** Запрет на вмешательство в личную жизнь или дела частного лица, если в результате этого вмешательства производятся чрезмерные или противозаконные накопление и использование данных этого лица.

uz – норасмийлик
en – privacy

2.1.19 **событие:** Наблюдаемое явление, которое невозможно предсказать (целиком) или которым невозможно управлять.

uz – ҳодиса
en – event

2.1.20 **событие информационной безопасности:** Идентифицированный случай состояния системы или сети, указывающий на возможное нарушение политики информационной безопасности или отказ средств защиты, либо ранее неизвестная ситуация, которая может быть существенной для безопасности.

uz – ахборот хавфсизлиги ҳодисаси
en – event of information security

2.1.21 **средства вычислительной техники**; СВТ: Совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

uz – ҳисоблаш техникаси воситалари; ҲТВ
en – facilities of computing machinery

O'ZSTANDART
STANDARTLASHTIRISH
MAZORATINI
AXBOROT

2.1.22 **субъект:** Активный логический объект, имеющий доступ к объектам.

uz – субъект
en – subject

Примечания

1 Активным логическим объектом может быть процесс, который запускает выполнение программы.

2 Субъект может быть причиной потока информации между объектами или изменения состояния системы обработки данных.

2.1.23 **технические средства информатизации; ТСИ:** Комплекс технических средств или отдельно установленные технические средства (в том числе средства вычислительной техники и другие устройства), предназначенные для обработки информации.

uz – ахборотлаштириш техник воситалари; АТВ
en – technical facilities of informatization

2.2 Характеристики безопасности информации

2.2.1 **аутентичность;** *подлинность*: Свойство, гарантирующее, что субъект или ресурс идентичны заявленным.

uz – аслига тўғрилик, ҳақиқийлик
en – authenticity

2.2.2 **достоверность:** Свойство данных на выходе системы соответствовать данным, поступившим на ее вход.

uz – ишончлилик
en – reliability

2.2.3 **доступность:** Состояние информации и её носителя, при котором обеспечивается беспрепятственное и своевременное получение пользователями предназначенной для них информации.

uz – фойдалана олишлик
en – availability

2.2.4 **конфиденциальность:** Состояние информации и ее носителя, при котором обеспечиваются предотвращение несанкционированного ознакомления с ней или несанкционированного документирования (снятия копий).

uz – конфиденциаллик
en – confidentiality

2.2.5 **неотказуемость:** Способность удостоверять имевшее место действие или событие так, чтобы эти события или действия не могли быть позже отвергнуты.

uz – рад этолмаслик
en – non-repudiation

Примечание – Под термином «неотказуемость» подразумевается, что ни один из взаимодействующих логических объектов не может отрицать свое участие в обмене данными.

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, METROLOGIYA
VA SERTIFIKATLASHTIRISH MARKAZI
AXBOROT TEXNIK VOSITALARI
JORIY ETISH BO'LIMI

2.2.6 **подотчетность:** Свойство, обеспечивающее однозначное отслеживание собственных действий любого логического объекта.

uz – ҳисоб беришлик
en – accountability

2.2.7 **целостность:** Состояние информации и ее носителя, при котором обеспечиваются неделимость и предотвращение несанкционированного или преднамеренного уничтожения, искажения, утечки, хищения, подделки, подмены в целом и ее отдельных составных частей.

uz – яхлитлик
en – integrity

2.2.8 **целостность системы:** Свойство системы обработки данных одновременно с выполнением своего оперативного предназначения предотвращать использование или модификацию ресурсов незарегистрированными пользователями, а также предотвращать использование или модификацию зарегистрированными пользователями не принадлежащих им ресурсов.

uz – тизимнинг яхлитлиги
en – system integrity

2.3 Требования по безопасности информации

2.3.1 **аттестация объектов информатизации:** Комплекс организационно-технических мероприятий, направленных на определение соответствия фактического состояния защищенности объектов информатизации требованиям государственных стандартов и нормативно-правовых актов в области информационной безопасности.

uz – ахборотлаштириш объектларини аттестатлаш
en – validation of objects of informatization

2.3.2 **задание по безопасности:** Совокупность требований безопасности и спецификаций, предназначенная для использования в качестве основы для оценки конкретного объекта.

uz – хавфсизлик бўйича топшириқ
en – security target

2.3.3 **класс защищенности средств вычислительной техники [автоматизированной системы]:** Определенная совокупность требований по защите средств вычислительной техники (автоматизированной системы) от несанкционированного доступа к информации.

uz – ҳисоблаш техникаси воситалари [автоматлаштирилган тизимнинг]нинг муҳофаза қилинганлик класси
en – security class of facilities of computing machinery [computer-based system]

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH ... INSTITUTI
MAZKURATINI ... NUSXASI
AXBOROT TEXNOLOGIYALARI ...

2.3.4 **модель защиты:** Абстрактное (формализованное или неформализованное) описание комплекса программно-технических средств и/или организационных мер защиты от несанкционированного доступа.

uz – муҳофаза қилиш модели
en – protection model

2.3.5 **показатели защищенности средств вычислительной техники [автоматизированной системы]:** Характеристика средств вычислительной техники (автоматизированной системы), влияющая на защищенность и описываемая определенной группой требований, варьируемых по уровню и глубине в зависимости от класса защищенности средств вычислительной техники (автоматизированной системы).

uz – ҳисоблаш техникаси воситалари [автоматлаштирилган тизимнинг]нинг муҳофаза қилинганлик кўрсатки-чи
en – protection criterions of facilities of computing machinery [computer-based system]

2.3.6 **политика безопасности:** Набор правил, определяющих процедуры и механизмы обеспечения безопасности заданного подмножества объектов и субъектов безопасности.

uz – хавфсизлик сиёсати
en – security policy

2.3.7 **профиль защиты:** Независимая от реализации совокупность требований безопасности для некоторой категории объектов, отвечающая специфическим запросам потребителя.

uz – муҳофаза қилиш профили
en – protection profile

2.3.8 **стратегия защиты:** Формальное определение критериев, особенно оперативных, которыми следует руководствоваться при обеспечении защиты системы от известных угроз.

uz – муҳофаза қилиш стратегияси
en – protection strategy

2.3.9 **уровень безопасности:** Совокупность иерархического грифа секретности и категории безопасности, которая указывает на чувствительность объекта к категории допуска лица.

uz – хавфсизлик даражаси
en – security level

2.3.10 **эшелонированная защита:** Концепция системы безопасности, при которой каждая подсистема в сети защищается до максимально возможного уровня.

uz – бирин-кетин жойлаштириб муҳофаза килиш
en – defence-in-depth

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, SIFAT
VA SERTIFIKATLASHTIRISH DAVLAT
AXBOROT TEXNOLOGIYALARI
JORIY ETISH BO'LIMI

2.4 Управление информационной безопасностью

2.4.1 **администратор безопасности [защиты]:** 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 Субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации.

uz – хавфсизлик [муҳофаза қилиш] маъмури
en – security administrator

2.4.2 **администрация системы защиты:** Орган управления, устанавливающий политику безопасности и определяющий объекты и субъекты, к которым данная политика применяется.

uz – муҳофаза қилиш тизимининг маъмурий бошқаруви
en – security system administration

2.4.3 **аудит безопасности:** Независимый просмотр и анализ записей системы обработки данных и ее работы для проверки на адекватность управляющих функций системы, обеспечения соответствия принятой политике безопасности и операционным процедурам, обнаружения нарушений безопасности и выдачи рекомендаций по любым определенным изменениям в управлении, политике безопасности и процедурах.

uz – хавфсизлик аудити
en – security audit

2.4.4 **сертификация:** Процедура, посредством которой третья сторона гарантирует, что вся система обработки данных или ее часть соответствует требованиям безопасности.

uz – сертификатлаш
en – certification

2.4.5 **система защиты информации от несанкционированного доступа;** СЗИ НСД: Комплекс организационных мер и программно-технических (в том числе криптографических) средств защиты от несанкционированного доступа к информации в автоматизированных системах.

uz – ахборотни рухсатсиз фойдалана олишдан муҳофаза қилиш тизими; АРФМТ
en – protection system of information from unauthorized access

2.4.6 **система обеспечения информационной безопасности:** Совокупность правовых, организационных и технических мероприятий, средств и норм, направленных на предотвращение или существенное затруднение нанесения ущерба интересам собственника информации.

uz – ахборот хавфсизлигини таъминлаш тизими
en – information security system

2.4.7 **система управления информационной безопасностью; СУИБ:** Часть общей системы управления, основанная на использовании методов оценки бизнес-рисков, предназначенная для разработки, внедрения, функционирования, мониторинга, анализа, обслуживания и совершенствования информационной безопасности.

Примечание – Система управления включает организационную структуру, политики, планирование деятельности, распределение ответственности, правила, процедуры, процессы и ресурсы.

uz – ахборот хавфсизлигини бошқариш тизими; АХБТ
en – information security management system; ISMS

2.4.8 **служба обеспечения информационной безопасности:** Структурное подразделение, занимающееся разработкой, реализацией и контролем выполнения организационно-технических, аппаратно-программных и режимных мер обеспечения информационной безопасности.

uz – ахборот хавфсизлигини таъминлаш хизмати
en – service of information security

2.5 Безопасность информации

2.5.1 **безопасность информации [данных]:** 1 Интегральное свойство информации [данных] противостоять случайным или преднамеренным воздействиям (угрозам), наносящим ущерб собственнику информации.

Примечание - Характеристиками безопасности информации [данных] являются конфиденциальность, целостность и доступность, а также неотказуемость, подотчетность, аутентичность и достоверность.

2 Состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз.

uz – ахборот [маълумотлар] хавфсизлиги
en – security of information [data]

2.5.2 **документированная информация;** *документ*: Зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

uz – ҳужжатлаштирилган ахборот; ҳужжат
en – documented information; document

2.5.3 **защита информации [данных]:** Комплекс правовых, организационных и технических (программно-аппаратных) мероприятий, направленных на предотвращение или затруднение нанесения ущерба интересам собственника информации (данных).

uz – ахборотни [маълумотларни] муҳофаза қилиш
en – protection of information [data]

2.5.4 **защита информации от несанкционированного доступа:** Деятельность, направленная на предотвращение получения защищаемой информации заинтересованным субъектом с нарушением установленных нормативно-правовыми актами или собственником информации прав или правил доступа к защищаемой информации.

uz – ахборотни рухсат этилмаган тарзда фойдалана олишдан муҳофаза қилиш
en – protection of information from unauthori-zed access

2.5.5 **информация ограниченного доступа:** Документированная информация, содержащая сведения, составляющие государственные секреты и конфиденциальную информацию, доступ к которой ограничивается в соответствии с законодательством.

uz – фойдалана олиш чекланган ахборот
en – limited access information

2.5.6 **категория безопасности:** Неиерархическое группирование чувствительной информации, используемое для управления доступом к данным, более точного, чем при использовании только иерархического грифа секретности.

uz – хавфсизлик категорияси
en – security category

2.5.7 **конфиденциальная информация:** Документированная информация, не содержащая сведений, составляющих государственные секреты, доступ к которой ограничивается в соответствии с законодательством.

uz – конфиденциал ахборот
en – confidential information

2.5.8 **метка конфиденциальности:** Элемент информации, который характеризует конфиденциальность информации, содержащейся в объекте.

uz – конфиденциаллик белгиси
en – confidentiality mark

2.5.9 **чувствительная [критичная] информация**: Информация, подлежащая согласно законодательству защите, или определенная собственником как нуждающаяся в защите, потому что ее раскрытие, модификация, уничто-

uz – таъсирчан [критик] ахборот
en – sensitive information

жение или сокрытие нанесет ощутимый ущерб кому-то или чему-то.

2.5.10 **чувствительность;** *критичность*: Степень важности информации, определяемая ее владельцем и указывающая на необходимость ее защиты.

uz –таъсирчанлик, критиклик
en – sensitivity

2.6 Угрозы информационной безопасности

2.6.1 **агрегирование:** Получение чувствительной информации методом сбора и сопоставления информации меньшей чувствительности.

uz – агрегирлаш
en – aggregation

2.6.2 **активная угроза:** Любая угроза преднамеренного несанкционированного изменения состояния системы обработки данных.

Примечание – Примером активной угрозы является угроза, в результате реализации которой возможны модификация сообщений, вставка ложных сообщений, маскарад или отказ в обслуживании.

uz – актив таҳдид
en – active threat

2.6.3 **активный перехват информации:** Подключение нелегального устройства к линии телекоммуникаций с целью модифицировать или вставить данные.

uz – ахборотни актив тарзда тутиб олиш
en – active wiretapping

2.6.4 **анализ трафика:** Извлечение сведений посредством анализа открытой информации на основе наблюдения за потоками трафика (наличие, отсутствие, объем, направление и частота).

uz – трафикни таҳлил қилиш
en – traffic analysis

2.6.5 **анализ угроз:** Исследование действий и событий, которые могут неблагоприятно воздействовать на систему обработки данных.

uz – таҳдидларнинг таҳлили
en – threat analysis

2.6.6 **блокирование передачи информации [данных]:** Одно из нарушений из области безопасности информации, выражающееся в прекращении передачи или задержке информации на время, за которое она потеряет ценность для пользователя.

uz – ахборот [маълумотлар] узатилишини блокировкалаш
en – information [data] transmission blocking

O‘ZSTANDART AGENTLIGI
ST... HUJJATLASHTIRISH, ODILLAT
BASSLARI BO‘YICHA ... AXBOROT TARQATISH ...
...

2.6.7 **брешь;** *лазейка*: Ошибка при назначении полномочий, упущение при разработке, которые позволяют обойти или вывести из строя механизмы защиты.

uz – тешик, туйнук
en – flaw, loophole

2.6.8 **внешний дестабилизирующий фактор:** Дестабилизирующий фактор, источник которого расположен вне сети телекоммуникаций.

uz – дестабиллаштирувчи ташқи омил
en – external destabilizing factor

2.6.9 **внутреннее мошенничество:** Использование служащими своего служебного положения для получения выгоды лично или через третьих лиц путем передачи им технических сведений конфиденциального характера.

uz – ички фирибгарлик
en – internal fraud

2.6.10 **внутренний дестабилизирующий фактор**: Дестабилизирующий фактор, источник которого расположен внутри сети телекоммуникаций или ее элементов.

uz – дестабиллаштирувчи ички омил
en – internal destabilizing factor

2.6.11 **вредоносная программа:** Программа, реализованная аппаратным, программно-аппаратным или программным способом и предназначенная для выполнения каких-либо несанкционированных или злоумышленных действий.

Примечание – Примерами вредоносных программ являются логическая бомба, троянская программа, вирус, червь.

uz – зарарловчи дастур
en – malicious logic

2.6.12 **временная бомба:** Логическая бомба, которая может быть активизирована в определенное время.

uz – вақт бомбаси
en – time bomb

2.6.13 **вход между строк:** Доступ, полученный нарушителем посредством активного перехвата при кратковременном выключении канала передачи данных, связанного с ресурсами законного пользователя.

uz – сатрлар орасига кириш
en – between-the-lines entry

2.6.14 **дестабилизирующее воздействие:** Действие, источником которого является физический или технологический процесс внутреннего или внешнего по отношению к сети телекоммуникаций характера, приводящее к выходу из строя элементов сети.

uz – дестабиллаштирувчи таъсир
en – destabilizing impact

2.6.15 **дестабилизирующий фактор:** Воздействие на сеть телекоммуникаций, источником которого является физический или технологический процесс внутреннего или внешнего по отношению к сети телекоммуникаций характера, приводящее к выходу из строя элементов сети.

uz – дестабиллаштирувчи омил
en – destabilizing factor

2.6.16 **доступ при отказе:** Несанкционированный и, как правило, случайный доступ к данным в системе обработки данных, ставший возможным в результате отказа оборудования или программного обеспечения.

uz – рад этиш вақтидаги фойдаланиш
en – failure access

2.6.17 **загрязнение:** Введение данных с одним грифом секретности или категорией безопасности в данные с более низким грифом секретности или другой категорией безопасности.

uz – ифлосланиш
en – contamination

2.6.18 **закладочное устройство:** Элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

uz – ўрнатилган қурилма
en – bug device

2.6.19 **искажение информации:** Случайная или преднамеренная несанкционированная модификация информации при ее обработке (передаче) техническими средствами в результате внешних воздействий (помех), сбоев в работе аппаратуры или ошибочных действий обслуживающего персонала.

uz – ахборотнинг бузилиши
en – information distortion

2.6.20 **клонирование:** Неправомочное изготовление телефонов или платежных телефонных карт с фальшивыми идентификаторами абонентов, номеров и платежных отметок.

uz – клонлаш
en – cloning

2.6.21 **компоновка;** *обобщение*: Целенаправленное объединение данных или информации одной системы обработки данных с данными или информацией другой системы для получения защищенной информации.

uz – компоновка қилиш, умумлаштириш
en – linkage, fusion

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH INSTITUTI
MAXSUS FOYDALANISH UCHUN
AXBOROT TEXNOLOGIYALARI
JORIY ETISH BILAN BOG‘LIQ

2.6.22 **компрометация:** Раскрытие криптографических ключей или конфиденциальной информации.

uz – компрометация (обрўсизлантириш)
en – compromise

2.6.23 **компьютерное злоупотребление:** Умышленное или случайное несанкционированное действие, которое влияет на компьютерную безопасность системы обработки данных или нарушает ее.

uz – компьютер суиистеъмоллиги
en – computer abuse

2.6.24 **компьютерное мошенничество:** Мошенничество, совершенное с помощью или при непосредственном использовании системы обработки данных или компьютерной сети.

uz – компьютер фирибгарлиги
en – computer fraud

2.6.25 **компьютерное преступление:** Преступление, совершенное с помощью или при непосредственном использовании системы обработки данных или компьютерной сети.

uz – компьютер жинояти
en – computer crime

2.6.26 **компьютерный взлом:** Несанкционированное проникновение в компьютерную сеть или в чужой компьютер с целью, например, извлечения выгоды, использования чужих данных, удовлетворения личного любопытства.

uz – компьютер воситасида бузиш (кириш)
en – cracking

2.6.27 **логическая бомба:** Вредоносная программа, запуск которой происходит при некотором определенном состоянии системы обработки данных и вызывает повреждение этой системы.

uz – мантиқий бомба
en – logic bomb

2.6.28 **люк:** Скрытый программный или аппаратный механизм, обычно создаваемый для тестирования и поиска неисправностей, который позволяет обойти механизмы компьютерной безопасности.

uz – люк
en – trapdoor

2.6.29 **маскарад:** Попытка какого-либо логического объекта выдать себя за другой логический объект для получения несанкционированного доступа.

uz – маскарад
en – masquerade

2.6.30 **модель угроз:** Физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

uz – таҳдидлар модели
en – threat model

MAZKUR HUJJATNING NUSXASI O'ZBEKISTON

2.6.31 **модификация информации:** Несанкционированное изменение содержания или объема информации на ее носителях при обработке техническими средствами.

uz – ахборотни ўзгартириш
en – information modification

2.6.32 **мошенничество:** Любые незаконные преднамеренные действия, связанные с использованием услуг телекоммуникаций без надлежащей оплаты, с целью получения выгоды.

uz – фирибгарлик
en – fraud

2.6.33 **нарушение защиты:** Обход системы компьютерной безопасности или вывод из строя какого-либо ее элемента, результатом которого может быть проникновение в систему обработки данных.

uz – муҳофаза қилишнинг бузилиши
en – breach

2.6.34 **незащищенность:** Возможность использования конкретной уязвимости системы обработки данных при проведении конкретной атаки.

uz – муҳофаза қилинмаганлик
en – exposure

2.6.35 **несанкционированное действие:** Действие в нарушение установленных правил.

uz – рухсатсиз фаолият
en – unauthorized action

2.6.36 **несанкционированный доступ; НСД:** Доступ субъекта к объекту или информации в нарушение установленных в системе правил разграничения доступа.

uz – рухсатсиз фойдалана олиш; РФО
en – unauthorized access

2.6.37 **обман:** Выполнение действий, направленных на введение в заблуждение пользователя, наблюдателя, например, оператора перехвата сообщений или ресурса.

uz – алдов
en – operator spoof

2.6.38 **отказ в обслуживании:** Прекращение санкционированного доступа к ресурсам или задержка выполнения операций, критичных по времени.

uz – хизмат кўрсатишни рад этиш
en – denial of service

2.6.39 **пассивная угроза:** Угроза несанкционированного раскрытия содержания информации без изменения состояния системы обработки данных.

uz – пассив таҳдид
en – passive treat

Примечание – Примером пассивной угрозы является угроза, в результате реализации которой возможно восстановление чувствительной информации из перехваченных передаваемых данных.

2.6.40 **пассивный перехват информации:** Подключение нелегального устройства к линии телекоммуникаций для получения данных.

uz – ахборотни пассив тарзда тутиб олиш
en – passive wiretapping

2.6.41 **переполнение:** Случайный или умышленный ввод большого объема данных, результатом которого является отказ в обслуживании.

uz – тўлдириш
en – flooding

2.6.42 **перехват информации:** Тайное подключение нелегального устройства к какой-либо части линии телекоммуникаций, чтобы получать, модифицировать или вставлять данные.

uz – ахборотни тутиб олиш
en – wiretapping

2.6.43 **побочное излучение:** Нежелательно излучаемые сигналы, при перехвате и анализе которых может быть раскрыта обрабатываемая или передаваемая чувствительная информация.

Примечание – Например, побочными излучениями могут быть акустические и электромагнитные излучения.

uz – номақбул нурланиш
en – compromising emanation

2.6.44 **подделка информации:** Умышленная несанкционированная модификация информации при ее обработке техническими средствами с целью получения определенных выгод (преимуществ) перед конкурентом или нанесения ему ущерба.

uz – ахборотни сохталаштириш
en – data falsification

2.6.45 **подстановка [заполнение] трафика:** Генерирование ложных событий связи, ложных блоков данных и/или ложных данных в блоках данных.

uz – трафикни ўрнига қўйиш [тўлдириш]
en – traffic padding

2.6.46 **почтовый червь:** Программа, которая способна рассылаться самостоятельно по электронной почте всем адресатам каждого списка доставки.

uz – почта қурти
en – email-worm

2.6.47 **преднамеренные угрозы:** Угрозы от случайного просмотра с использованием легко доступных инструментов слежения до изощренных попыток нарушения защиты с использованием специальных знаний о системе.

uz – қасддан қилинадиган таҳдидлар
en – intentional threats

O'ZSTANDART AGENTLIGI
STANDARTLAR ...
NAZORATI ...
AXBOROT ...
JORIY ETILGAN ...

2.6.48 **прерывание соединения:** Разъединение, производимое в нарушение установленных процедур.

Примечание - Прерывание соединения может дать возможность другим логическим объектам получить несанкционированный доступ.

uz – боғланишни узиш
en – aborted connection

2.6.49 **программная закладка:** Преднамеренно внесенные в программное обеспечение функциональные объекты, которые при определенных условиях (входных данных) инициируют выполнение не описанных в документации функций программного обеспечения, приводящих к нарушению конфиденциальности, доступности или целостности информации.

uz – дастурий ўрнатма
en – software bug

2.6.50 **программное пиратство:** Неправомерное использование, копирование или распространение программных продуктов, являющихся авторским произведением.

uz – дастурий қароқчилик
en – software piracy

2.6.51 **программный вирус;** *вирус*: Специально разработанная вредоносная программа, которая самопроизвольно размножается путем вставления своих возможно измененных копий в другие программы и модификации их при этом, и которая выполняется при вызове инфицированной программы.

Примечание – Вирус часто является причиной искажений или разрушений и, в некоторых случаях, может активизироваться при наступлении определенной даты.

uz – дастурий вирус, вирус
en – program virus, virus

2.6.52 **продажа вызовов:** Вид криминальной деятельности, при которой злоумышленник получает прибыль путем продажи дорогостоящих вызовов со значительными скидками, организуя нелегальные «переговорные пункты».

uz – чақирувларни сотиш
en – call selling

2.6.53 **проникновение:** Несанкционированный доступ к системе обработки данных.

uz – ичига кириб олиш
en – penetration

2.6.54 **прослушивание:** Перехват злоумышленником передаваемой по сети информации с целью выявления и последующего использования слабых мест системы защиты.

uz – эшитиш
en – eavesdropping

O'ZBEKISTON STANDARTI NUSXASI
SO'ZBEKISTAN STANDARTLARI AXBOROT FONDI NUSXASI

2.6.55 **процедурное мошенничество:** Неправомочное использование роуминга и других сетевых процедур (например, биллинга) с целью уменьшения оплаты услуг телекоммуникаций.

uz – процедура фирибгарлиги
en – procedural fraud

2.6.56 **прошивка сети:** Способ проникновения, при котором используются различные сети телекоммуникаций с целью получить доступ к системе обработки данных и при этом избежать обнаружения и определения местонахождения.

uz – тармоқни тешиб ўтиш
en – network weaving

2.6.57 **раскрытие:** Нарушение компьютерной безопасности, в результате которого данные становятся доступны неполномочным логическим объектам.

uz – фош этиш
en – disclosure

2.6.58 **распределенный отказ в обслуживании:** Нарушение работы сети, обусловленное одновременной атакой злоумышленников на разные ее элементы, производимой с большого числа компьютеров.

uz – хизмат кўрсатишни тақсимланган рад этиш
en – distributed denial of service

2.6.59 **рассылка спама:** Рассылка незапрашиваемых данных, которые перегружают систему.

uz – спамни жўнатиш
en – spamming

2.6.60 **сбор мусора:** Выполнение несанкционированного поиска остаточных данных для получения чувствительной информации.

uz – ахлат йиғиш
en – garbage collection

2.6.61 **скрытый канал:** Канал передачи, который может быть использован для передачи данных способом, нарушающим политику безопасности.

uz – яширин канал
en – covert channel

2.6.62 **случайные угрозы:** Угрозы, не связанные с умышленным намерением. Например, нарушения работы системы, грубые эксплуатационные ошибки и ошибки в программном обеспечении.

uz – тасодифий таҳдидлар
en – accidental threats

O'ZSTANDART
STANDART
MASTER

2.6.63 **социальная инженерия:** Метод несанкционированного доступа к информации или системам хранения информации без использования технических средств, основанный на знании человеческой природы, особенностях принятия решения людьми и социальной психологии.

uz – ижтимоий инженерия
en – social engineering

2.6.64 **троянская программа:** Вредоносная программа, выглядящая как функционально полезная, позволяющая производить несанкционированный сбор, фальсификацию или уничтожение данных.

uz – троян дастури
en – trojan

2.6.65 **угроза**: Потенциальная возможность нарушения компьютерной безопасности.

uz – таҳдид
en – threat

2.6.66 **уничтожение информации:** Случайное или умышленное стирание информации на ее носителях при обработке техническими средствами.

uz – ахборотни йўқ қилиш
en – data destruction

2.6.67 **ущерб:** Количественная мера ущерба или убытка, полученного в результате компрометации.

uz – зарар
en – loss

2.6.68 **уязвимость:** Недостаток в системе обработки данных, используя который, можно нарушить её целостность и вызвать неправильную работу.

uz – заифлик
en – vulnerability

Примечания

1 Уязвимость может быть результатом ошибок программирования, недостатков, допущенных при проектировании системы, ненадежных паролей, воздействия вирусов или других вредоносных программ и т.п.

2 Если при наличии уязвимости имеется соответствующая угроза, то существует и риск.

2.6.69 **уязвимость информации:** Подверженность информации воздействию различных дестабилизирующих факторов, которые могут привести к нарушению ее конфиденциальности, целостности, доступности или неправомерному тиражированию.

uz – ахборотнинг заифлиги
en – vulnerability of information

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH INSTITUTI
MILLIY STANDARTLARNI TARQATISH BO‘LIMI
Axborot Texnologiyalari
Jamiyat Evolyutsiyasi

2.6.70 **фактор, воздействующий на защищаемую информацию**: Явление, действие или процесс, результатом которых могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней.

uz – муҳофаза қилинадиган ахборотга таъсир кўрсатувчи омил
en – factor, acting upon protectable information

2.6.71 **физическая угроза:** Угроза, последствием реализации которой является физический ущерб всей системе.

uz – жисмоний таҳдид
en – physical threat

2.6.72 **физический пиггибекинг:** Несанкционированный проход через контролируемую дверь вслед за полномочным лицом.

uz – жисмоний пиггибекинг
en – to tailgate

2.6.73 **червь:** Независимая программа, способная самостоятельно распространяться в системах обработки данных или компьютерных сетях.

Примечание – Черви часто разрабатываются, чтобы использовать доступные ресурсы, например, объем памяти или время обработки.

uz – қурт
en – worm

2.6.74 **эксплуатационный люк:** Люк в программном обеспечении, который облегчает обслуживание, предоставляя дополнительные возможности для входа в программу в недокументированных точках или без обычных проверок.

uz – эксплуатация қилиш люки
en – maintenance hook

2.6.75 **электронный пиггибекинг:** Несанкционированный доступ к системе обработки данных по легальному соединению полномочного пользователя.

uz – электрон пиггибекинг
en – piggyback entry

2.7 Риски

2.7.1 **анализ рисков:** Систематическое выполнение процедур идентификации ресурсов системы обработки данных, угроз этим ресурсам и уязвимостей системы к этим угрозам.

uz – риск таҳлили
en - risk analysis

2.7.2 **базовый анализ рисков:** Анализ рисков, проводимый в соответствии с требованиями базового уровня информационной безопасности.

uz – рискларнинг асосий таҳлили
en – baseline risk analysis

2.7.3 **идентификация риска:** Процесс определения, составления перечня и описания риска.

Примечания

1 Идентификация риска может включать в себя источники риска, события, их причины и возможные последствия.

2 Идентификация риска может также включать в себя теоретический анализ, анализ хронологических данных, экспертных оценок и потребностей заинтересованных сторон.

uz – рискни идентификация қилиш
en – risk identification

2.7.4 **критерии риска:** Признаки, по которым оценивают значимость риска.

Примечания

1 Критерии риска основываются на целях организации, а также на внешней и внутренней ситуации.

2 Критерии риска могут быть взяты из стандартов, законов, политик и других требований.

uz – риск мезонлари
en – risk criteria

2.7.5 **обработка рисков:** Процесс выбора и внедрения мер по изменению рисков.

uz – рискни қайта ишлаш
en – risk treatment

2.7.6 **определение рисков:** Процесс, включающий анализ и оценку рисков.

uz – рискларни аниқлаш
en – risk assessment

2.7.7 **остаточный риск:** Риск, остающийся после его обработки.

uz – қолдиқ риск
en – residual risk

2.7.8 **оценка рисков:** Процесс сравнения рассчитанного риска и критериев риска, выполняемый с целью определения его значения.

uz – рискларни баҳолаш
en – risk evaluation

2.7.9 **полный анализ рисков:** Анализ рисков для информационных систем, предъявляющих повышенные требования в области информационной безопасности (более высокие, чем базовый уровень информационной безопасности).

Примечание – Полный анализ рисков предполагает определение ценности ресурсов, оценку угроз и уязвимостей, выбор адекватных контрмер и оценку их эффективности.

uz – рискларни тўлиқ таҳлил қилиш
en – full risk analysis

2.7.10 **принятие риска:** Решение администрации считать приемлемым некоторый уровень риска, как правило, по техническим или финансовым причинам.

uz – рискни қабул қилиш
en – risk acceptance

2.7.11 **процесс управления риском:** Взаимосвязанные действия по обмену информацией, консультациям, установлению целей, области применения, идентификации, исследованию, оценке, обработке, мониторингу и анализу риска, выполняемые в соответствии с политикой, процедурами и методами управления организации.

uz – рискни бошқариш жараёни
en – risk management process

2.7.12 **риск:** Возможность использования конкретной уязвимости системы обработки данных при реализации конкретной угрозы.

uz – риск
en – risk

2.7.13 **управление рисками:** Координированная деятельность по руководству и управлению организацией по отношению к риску.

Примечание - Управление рисками обычно включает определение рисков, обработку рисков, принятие рисков и сообщение о рисках.

uz – рискларни бошқариш
en – risk management

2.7.14 **уровень риска:** Величина риска, характеризуемая сочетанием последствий и их вероятности.

uz – риск даражаси
en – level of risk

2.8 Атаки

2.8.1 **активная атака:** Реализация активной угрозы безопасности.

uz – фаол ҳужум
en – active attack

2.8.2 **аналитическая атака;** *криптоаналитическая атака*: Попытка разгадать код или найти ключ, используя аналитические методы.

Примечания

1 Аналитическая атака является противоположностью атаки на основе полного перебора.

2 Примерами аналитических атак являются статистический анализ изображений, поиск недостатков в алгоритме шифрования.

uz – аналитик ҳужум, криптоаналитик ҳужум
en – analytical attack, cryptanalytical attack

2.8.3 **атака:** Действия, предпринимаемые в целях обхода механизмов обеспечения безопасности или в целях использования их недостатков.

uz – ҳужум
en – attack

2.8.4 **атака перебором открытого текста**: Аналитическая атака, когда криптоаналитик может рассматривать неограниченное количество открытого текста сообщения и исследовать соответствующий шифротекст.

uz – очиқ матнни ажратиб бажариладиган ҳужум
en – chosen-plaintext attack

2.8.5 **атака переполнения:** Создание искусственной перегрузки сетевого оборудования (маршрутизаторов, коммутаторов и др.) за счет введения ложного трафика большого объема.

uz – тўлдириб юбориш ҳужуми
en – flooding attack

2.8.6 **атака по известному открытому тексту:** Аналитическая атака, когда криптоаналитик располагает шифротекстом и значительным количеством соответствующего ему открытого текста.

uz – маълум очиқ матн бўйича ҳужум
en – known-plaintext attack

2.8.7 **атака полным перебором;** *лобовая атака*: Попытка нарушить компьютерную безопасность методом проб и ошибок, перебирая возможные значения паролей или ключей.

Примечание – Атака полным перебором является противоположностью аналитической атаки.

uz – тўлиқ ажратиб бажариладиган ҳужум, рўпарадан қилинган ҳужум
en – exhaustive attack, brute-force attack

2.8.8 **атака типа «отказ в обслуживании»:** Преднамеренное воздействие на информационную систему или оборудование с целью создания условий, при которых правомерные пользователи не могут получить доступ к предоставляемым системой или оборудованием ресурсам или такой доступ им будет затруднен.

uz – «хизмат кўрсатишни рад этиш» туридаги ҳужум
en – denial of service attack

2.8.9 **атака только по шифротексту:** Аналитическая атака, когда криптоаналитик располагает только шифротекстом.

uz – фақат шифрланган матн бўйича ҳужум
en – ciphertext-only attack

2.8.10 **внутренняя атака:** Атака, выполняемая из самой защищенной сети.

uz – ички ҳужум
en – insider attack

2.8.11 **замещение:** Вид атаки, при которой сообщение запоминается и позднее передается вновь, замещая или повторяя первоначальное сообщение.

uz – ўрнини босиш
en – replay attack

2.8.12 **косвенная атака:** Попытка нарушения защиты системы, основанная на обходе механизма обеспечения безопасности или принуждении системы к неправильному использованию этого механизма.

uz – билвосита ҳужум
en – indirect attack

O‘ZBEKISTON STANDARTLARI

2.8.13 **неавторизованная попытка доступа к информации:** Попытка получить доступ к информации за счет обхода (обмана) средств контроля доступа в сети.

uz – ахборотдан муаллифлаштирилмаган тарзда фойдаланишга уриниш
en – attempt of unauthorised access to information, hacking

2.8.14 **недекларированные возможности:** Функциональные возможности программного обеспечения, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

uz – декларация қилинмаган имкониятлар
en – undocumented features

2.8.15 **непосредственная атака:** Попытка нарушения защиты системы, основанная на недостатках базовых алгоритмов, принципов или свойств механизма обеспечения безопасности.

uz – бевосита ҳужум
en – direct attack

2.8.16 **пассивная атака:** Атака, при которой нарушитель не имеет возможности модифицировать передаваемые сообщения и вставлять в информационный канал между отправителем и получателем свои сообщения.

Примечание - Целью пассивной атаки может быть только прослушивание передаваемых сообщений и анализ трафика.

uz – пассив ҳужум
en – passive attack

2.8.17 **спуфинг:** Вид сетевой атаки, когда злоумышленник пытается войти в защищенную сеть, используя ложный сетевой адрес.

uz – спуфинг
en – spoofing

2.9 Управление доступом

2.9.1 **авторизация:** Проверка прав доступа пользователя и получение им доступа к ресурсам в соответствии с данными ему правами.

Примечание – Авторизации обычно предшествует процедура аутентификации.

uz – муаллифлаштириш
en – authorization

2.9.2 **авторизованный субъект доступа:** Субъект, которому предоставлены соответствующие права доступа к объектам системы (полномочия).

uz – муаллифлаштирилган эркин фойдаланиш субъекти
en – authorized access subject

2.9.3 **аппаратный токен:** Компактное устройство, используемое для идентификации его владельца, безопасного удаленного доступа к информационным ресурсам.

Примечание – К аппаратным токенам относятся смарт-карта, брелок.

uz – аппаратли токен
en – hard token

2.9.4 **аутентификация:** Процедура установления подлинности пользователя (абонента сети, отправителя сообщения), программы, устройства или данных (информации, получаемого сообщения, ключа).

uz – аутентификация қилиш
en – authentication

2.9.5 **аутентификация личности;** *подтверждение подлинности личности*: Выполнение проверок (например, пароля или токена), позволяющих системе обработки данных распознавать логические объекты.

uz – шахсни аутентификация қилиш, шахснинг ҳақиқийлигини тасдиқлаш
en – identity authentication, identity validation

2.9.6 **аутентификация сообщения:** Верификация того, что сообщение заявленного отправителя было передано предназначенному получателю неповрежденным и неизмененным.

uz – хабарни аутентификация қилиш
en – message authentication

2.9.7 **верительные данные:** Данные, передаваемые для установления заявленной подлинности логического объекта.

uz – ишончли маълумотлар
en – credentials

2.9.8 **вид доступа:** Вид операции, указанной в праве на доступ.

Примечание – В праве на доступ могут быть указаны следующие операции: чтение, запись, выполнение, дополнение, модификация, удаление, создание.

uz – фойдаланиш тури
en – access type

2.9.9 **дискреционное управление доступом:** Разграничение доступа между поименованными субъектами и поименованными объектами.

Примечание - Субъект с определенным правом доступа может передать это право любому другому равноправному субъекту.

uz – фойдаланишни дискрецион бошқариш
en – discretionary access control

2.9.10 **диспетчер доступа;** *ядро защиты*: Аппаратные, программные и программно-аппаратные элементы комплекса средств защиты, реализующие концепцию диспечера доступа.

uz – фойдалана олиш диспетчери, муҳофаза қилиш ядроси
en – reference monitor, security kernel

2.9.11 **доступ:** Специальный тип взаимодействия между субъектом и объектом, в результате которого создается поток информации от одного к другому.

uz – фойдалана олиш
en – access

2.9.12 **доступ к информации:** Ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации.

uz – ахборотдан фойдалана олиш
en – access to information

2.9.13 **доступ к информационному ресурсу:** Получение субъектом доступа возможности манипулировать (использовать, управлять, изменять характеристики и т.п.) данными информационных ресурсов.

uz – ахборот ресурсидан фойдалана олиш
en – access to information resource

2.9.14 **доступ на запись:** Право на доступ, при получении которого разрешается записывать данные.

Примечание - Доступ на запись является разрешением на дополнение, модификацию, удаление или создание данных.

uz – ёзиб олишга рухсат
en – write access

2.9.15 **доступ на чтение:** Право на доступ, при получении которого разрешается читать данные.

uz – ўқиш учун рухсат
en – read access

2.9.16 **идентификатор:** Символ или последовательность символов (сигналов) для обозначения ими наименования определенной совокупности сведений.

uz – идентификатор
en – identifier

2.9.17 **идентификатор доступа:** Уникальный признак субъекта или объекта доступа.

uz – фойдалана олиш идентификатори
en – access identifier

2.9.18 **идентификатор пользователя:** Последовательность символов или изображение, которые используются системой обработки данных для идентификации пользователя.

uz – фойдаланувчининг идентификатори
en – user identifier

2.9.19 **идентификация:** Присвоение субъектам и объектам доступа идентификатора и/или сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

uz – идентификация қилиш
en – identification

2.9.20 **идентификация терминала:** Процесс автоматической передачи на абонентский терминал установленного идентификатора, относящегося к удаленному абонентскому терминалу (терминалам), с которым (которыми) установлено соединение.

uz – терминални идентификация қилиш
en – terminal identification

2.9.21 **информация аутентификации:** Информация, используемая для установления достоверности идентификационной информации, предъявленной логическим объектом.

uz – аутентификация қилиш ахбороти
en – authentication information

2.9.22 **категория допуска;** *допуск*: Разрешение, выданное лицу на право доступа к данным или информации заданного или более низкого уровня безопасности.

uz – рухсат бериш тоифаси, рухсат бериш
en – security clearance, clearance

2.9.23 **категория доступа:** Категория, присваиваемая логическим объектам, на основании которой они получают разрешение на использование ресурсов.

uz – фойдалана олиш категорияси
en – access category

2.9.24 **концепция диспечера доступа:** Концепция управления доступом, относящаяся к абстрактной машине, которая посредничает при всех обращениях субъектов к объектам.

uz – фойдалана олиш диспетчери концепцияси
en – reference monitor concept

2.9.25 **логическое управление доступом:** Использование механизмов, обеспечивающих управление доступом к данным или информации.

Примечание – Как правило, для логического управления доступом используется пароль.

uz – фойдаланишни мантиқий бошқариш
en – logical access control

2.9.26 **мандат:** Предоставление одного или нескольких прав на доступ к объекту.

Примечание - Мандат является разрешением на доступ.

uz – мандат
en – ticket

2.9.27 **мандатное управление доступом:** Разграничение доступа субъектов к объектам, основанное на назначении метки конфиденциальности для информации, содержащейся в объектах, и выдаче официальных разрешений (допуска) субъектам на обращение к информации такого уровня конфиденциальности.

uz – фойдалана олишни мандатли бошқариш
en – mandatory access control

2.9.28 **матрица доступа:** Таблица, отображающая права разграничения доступа.

uz – фойдалана олиш матрицаси
en – access matrix

2.9.29 **минимум привилегий:** Наделение субъектов только теми правами на доступ, которые им необходимы для выполнения конкретных задач.

uz – имтиёзлар минимуми
en – minimum privilege

2.9.30 **модель нарушителя правил разграничения доступа:** Абстрактное (формализованное или не формализованное) описание нарушителя правил разграничения доступа.

uz – фойдалана олишни чегаралаш қоидаларини бузувчининг модели
en – security policy violator model

2.9.31 **нарушитель правил разграничения доступа:** Субъект доступа, осуществляющий несанкционированный доступ к информации.

uz – фойдалана олишни чегаралаш қоидаларини бузувчи
en – security policy violator

2.9.32 **несанкционированный доступ к информации:** Доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Примечание – Под штатными средствами понимается совокупность программного, программно-аппаратного и аппаратного обеспечения средств вычислительной техники или автоматизированных систем.

uz – ахборотдан рухсатсиз фойдана олиш
en – unauthorized access to information

2.9.33 **обмен аутентификацией:** Механизм, предназначенный для подтверждения подлинности какого-либо логического объекта путем обмена информацией.

uz – аутентификация билан алмашиш
en – authentication exchange

2.9.34 **объект доступа:** Единица информационного ресурса системы, доступ к которой регламентируется правилами разграничения доступа.

uz – фойдалана олиш объекти
en – access object

2.9.35 **пароль:** Идентификатор субъекта доступа, являющийся его (субъекта) секретом.

uz – парол
en – password

STANDARTLAR
MAHSULOT
AXBOROT

2.9.36 **период доступа:** Временной интервал, в течение которого действуют права доступа.

uz – фойдалана олиш даври
en – access period

2.9.37 **политика управления доступом:** Набор правил, определяющих условия, при которых доступ может иметь место.

uz – фойдалана олишни бошқариш сиёсати
en – access control policy

2.9.38 **полномочие:** Представление идентификации объекта или класса объектов и всех разрешенных видов доступа к этим объектам.

Примечание – Полномочие может быть реализовано в форме мандата.

uz – ваколат
en – capability

2.9.39 **правила разграничения доступа:** Совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

uz – фойдалана олишни чеклаш қоидалари
en – security policy

2.9.40 **право доступа к записи:** Предоставление субъекту полномочий на запись (модификацию) определенной информации.

uz – ёзувдан фойдалана олиш ҳуқуқи
en – write access control

2.9.41 **право доступа к чтению:** Предоставление субъекту полномочий на чтение определенной информации.

uz – ўқиш имкониятини олиш ҳуқуқи
en – read access control

2.9.42 **право на доступ:** Разрешение субъекту на получение доступа к определенному объекту для выполнения операции определенного вида.

Примечание – Примером права на доступ является разрешение на чтение файла, но не на запись в него.

uz – фойдалана олиш ҳуқуқи
en – access right

2.9.43 **принцип «положено знать»:** Обоснованное требование предполагаемого получателя ознакомиться с необходимыми данными, получить к ним доступ или овладеть любой чувствительной информацией, содержащейся в этих данных.

uz – «билиш зарур» принципи
en – need-to-know

2.9.44 **программный токен:** Ключ для доступа к сервисам, выдаваемый пользователю после успешной авторизации.

uz – дастурий токен
en – soft token

O'ZSTANDART AGENTLIGI

2.9.45 **профиль пользователя:** Образец деятельности пользователя, который может использоваться для обнаружения изменений в его деятельности.

Примечание - Профиль пользователя может содержать такие данные как идентификатор пользователя, имя пользователя, пароль, права доступа и другие атрибуты.

uz – фойдаланувчининг профили
en – user profile

2.9.46 **разрешение на доступ:** Все права доступа субъекта к некоторому объекту.

uz – фойдаланишга рухсат
en – access permission

2.9.47 **регистрация деятельности:** Отслеживание действий субъекта доступа или злоумышленника в системе.

uz – фаолиятни қайд қилиш
en – activity registration

2.9.48 **регистрация пользователя:** Учет входа пользователя в систему с указанием кода идентификации или пароля для получения доступа в систему.

uz – фойдаланувчини рўйхатга олиш
en – user registration

2.9.49 **санкционированный доступ к информации:** Доступ к информации, не нарушающий установленные правила разграничения доступа.

uz – ахборотдан рухсат этилган тарзда фойдана олиш
en – authorized access to information

2.9.50 **система разграничения доступа;** СРД: Совокупность реализуемых правил разграничения доступа в средствах вычислительной техники или автоматизированных системах.

uz – фойдалана олишни чегаралаш тизими; ФЧТ
en – security policy realization

2.9.51 **система управления доступом;** СУД: Автоматизированные средства физического управления доступом.

Примечание – В СУД используются идентификационные карты с магнитной полосой, смарт-карты, считывающие биометрические устройства.

uz – фойдалана олишни бошқариш тизими; ФБТ
en – controlled access system; CAS

2.9.52 **список полномочий:** Ассоциированный с субъектом список, в котором указаны все виды доступа этого субъекта ко всем объектам.

Примечание - Для процесса, включенного в список, должны быть определены все виды доступа ко всем файлам и другим защищенным ресурсам.

uz – ваколатлар рўйхати
en – capability list

2.9.53 **список управления доступом:** Список логических объектов, имеющих полномочия на получение доступа к ресурсу, вместе с перечнем их прав доступа.

uz – фойдалана олишни бошқариш рўйхати
en – access control list

2.9.54 **субъект доступа:** Лицо или процесс, действия которых регламентируются правилами разграничения доступа.

uz – фойдалана олиш субъекти
en – access subject

2.9.55 **точка доступа к сети:** Точка, в которой оператор сети предоставляет услуги пользователю, то есть точка разделения ответственности оператора и ответственности пользователя в условиях эксплуатации.

uz – тармоқдан фойдалана олиш нуқтаси
en – network access point

2.9.56 **управление доступом:** Методы, обеспечивающие возможность обращения к ресурсам системы обработки данных только уполномоченным логическим объектам и только разрешенным способом.

uz – фойдалана олишни бошқариш
en – access control

2.9.57 **уровень доступа:** Уровень полномочий, необходимый логическому объекту для получения доступа к защищенному ресурсу.

Примечание – Уровнем доступа могут быть полномочия на доступ к данным или информации заданного уровня безопасности.

uz – фойдалана олиш даражаси
en – access level

2.9.58 **уровень полномочий субъекта доступа:** Совокупность прав доступа субъекта доступа.

uz – фойдалана олиш субъектлари ваколатлари даражаси
en – subject privilege

2.9.59 **услуга управления доступом:** Способы, обеспечивающие доступ субъектов только разрешенным способом.

uz – фойдалана олишни бошқариш хизмати
en – access control service

2.9.60 **физическое управление доступом:** Использование физических механизмов, обеспечивающих управление доступом.

Примечание – Примером физического управления доступом является хранение компьютера в запираемом на замок помещении.

uz – фойдалана олишни жисмонан бошқариш
en – physical access control

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH DAVLAT
MILLIY AGENTLIGI

2.10 Методы защиты информации

2.10.1 **домен безопасности:** Совокупность пользователей, систем или ресурсов, подчиняющихся единой политике безопасности и единой администрации безопасности.

uz – хавфсизлик домени
en – security domain

2.10.2 **замкнутая безопасная среда:** Среда, в которой особое внимание уделяется защите данных и ресурсов от случайных или злоумышленных действий (в виде авторизации, категорий допусков, управления конфигурацией и т.д.).

uz – ёпиқ хавфсиз муҳит
en – closed-security environment

2.10.3 **защита от несанкционированного доступа:** Деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником (владельцем) информации прав или правил доступа к защищаемой информации.

uz – рухсатсиз фойдалана олишдан муҳофаза қилиш
en – protection from unauthorized access

2.10.4 **зона безопасности:** Пространство, в пределах которого обеспечивается требуемый уровень защиты информации.

uz – хавфсизлик зонаси
en – security zone

2.10.5 **криптографический метод защиты информации:** Метод защиты информации, основанный на принципах шифрования и/или электронной цифровой подписи.

Примечание - Криптографический метод может быть реализован программными, аппаратными и аппаратно-программными средствами.

uz – ахборотни муҳофаза қилишнинг криптографик усули
en – cryptographic method of information protection

2.10.6 **маскировка:** Метод защиты объектов, основанный на использовании действий, вследствие которых объект становится недоступным (скрытым) или труднодоступным для злоумышленников.

uz – ниқоблаш
en – masking

2.10.7 **многоуровневая защита:** Защита, обеспечивающая разграничение доступа субъектов с различными правами доступа к объектам различных уровней конфиденциальности.

uz – кўп поғонали муҳофаза қилиш
en – multilevel protection

2.10.8 **открытая безопасная среда:** Среда, в которой защита данных и ресурсов от случайных или злоумышленных действий достигается посредством нормальных операционных процедур.

uz – очиқ хавфсиз муҳит
en – open-security environment

2.10.9 **препятствие:** Метод организационного, технического, программного преграждения доступа к защищаемой информации и объекту.

uz – тўсқинлик
en – obstacle

2.10.10 **принуждение:** Метод защиты, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

uz – мажбурлаш
en – enforcement

2.10.11 **разделение:** Деление данных на изолированные блоки, управление безопасностью которых производится раздельно, с целью уменьшения риска.

Примечание – Для ограничения воздействия на весь проект производится разделение данных главного проекта на блоки, соответствующие разделам проекта, каждый из которых имеет собственную систему безопасности.

uz – ажратиш
en – compartmentalization

2.10.12 **регламентация:** Метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи защищаемой информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму.

uz – тартибга солиш
en – regulation

2.10.13 **способ защиты информации:** Порядок и правила применения определенных принципов и средств защиты информации.

uz – ахборотни муҳофаза қилиш усули
en – method of protection of information

2.10.14 **техническая защита информации:** Деятельность, направленная на обеспечение безопасности информации, инженерно-техническими и некриптографическими методами с использованием средств технической защиты информации.

uz – ахборотни техник мухофаза қилиш
en – technical protection of information

2.10.15 **экранирование:** Функция межсетевого экрана, позволяющая поддерживать безопасность объектов внутренней области, игнорируя несанкционированные запросы из внешней области.

uz – экранлаштириш
en – screening

2.11 Криптографические методы защиты информации

2.11.1 **ассимметричная криптография;** *криптография с открытым ключом*: Криптография, в которой для шифрования и дешифрования используется как открытый ключ, так и соответствующий ему личный ключ.

Примечание - Если открытый ключ используется для шифрования, то соответствующий ему личный ключ должен использоваться для дешифрования, и наоборот.

uz – асимметрик криптография, очиқ калитли криптография
en – asymmetric cryptography, public-key cryptography

2.11.2 **дешифрование;** *декодирование*: Процесс получения из шифротекста соответствующих исходных данных.

Примечание - Шифротекст может быть зашифрован вторично, в этом случае при первом дешифровании исходный открытый текст не может быть восстановлен.

uz – дешифрлаш, декодлаш
en – decryption, decipherment

2.11.3 **ключ:** Последовательность символов, управляющая операциями шифрования и дешифрования.

uz – калит
en – key

2.11.4 **криптоанализ:** Анализ криптографической системы и/или ее входов и выходов с целью получения чувствительной информации, включая открытый текст.

uz – криптотаҳлил
en – cryptanalysis

2.11.5 **криптографическая защита информации:** Комплекс мероприятий, направленных на обеспечение целостности, доступности и конфиденциальности информации, осуществляемый при помощи алгоритмов криптографического преобразования (криптоалгоритмов).

uz – ахборотни криптографик муҳофаза қилиш
en – cryptographic protection to information

2.11.6 **криптографическая система;** *система шифрования*; *криптосистема*: Совокупность организационных, технических и программных средств, обеспечивающих криптографическое преобразование информации и/или управление, в том числе автоматизированное,

uz – криптографик тизим, шифрлаш тизими, криптотизим
en – cryptographic system, ciphersystem, cryptosystem

процессом изготовления и распределения криптографических ключей.

2.11.7 **криптографический алгоритм;** *криптоалгоритм*: 1 Алгоритм преобразования данных, использующий в своей работе набор секретных и открытых параметров, публикуемый, как правило, в открытой печати. 2 Математический алгоритм преобразования информации (данных) с целью предотвращения возможности ее искажения и защиты от несанкционированного доступа.

uz – криптографик алгоритм; криптографик алмаштириш алгоритми
en – cryptographic algorithm

2.11.8 **криптография:** Дисциплина, охватывающая принципы, средства и методы преобразования данных для сокрытия их семантического содержимого, предотвращения их несанкционированного использования или необнаруживаемой модификации.

uz – криптография
en – cryptography

2.11.9 **личный ключ:** Ключ, предназначенный для дешифрования и используемый только его владельцем.

uz – шахсий калит
en – private key

2.11.10 **необратимое шифрование;** *необратимое кодирование*; *одностороннее шифрование*: Шифрование, результатом которого является шифротекст, исходные данные которого не могут быть восстановлены.

Примечание - Одностороннее шифрование используется для аутентификации. Например, полученный в результате шифрования пароля методом одностороннего шифрования шифротекст сохраняется. Пароль, представленный позже, будет зашифрован таким же образом. Затем оба полученных шифротекста сравниваются, и если они идентичны, то предъявлен верный пароль.

uz – қайтарилмайдиган шифрлаш, қайтарилмайдиган кодлаш, бир томонлама шифрлаш
en – irreversible encryption, irreversible encipherment, one-way encryption

2.11.11 **открытый ключ:** Ключ, который предназначен для использования любым логическим объектом для зашифрованной связи с владельцем соответствующего личного ключа.

uz – очиқ калит
en – public key

2.11.12 **открытый текст:** Данные, семантическое содержимое которых доступно без использования криптографических методов.

uz – очиқ матн
en – plaintext, cleartext

2.11.13 **перестановка:** Шифрование, при котором биты или символы переставляются по по некоторой схеме.

Примечание – Полученный шифротекст называется шифром перестановки.

uz – ўрнини алмаштириш
en – transposition

2.11.14 **подстановка:** Шифрование, при котором последовательность битов или символов заменяется другой последовательностью битов или символов.

Примечание – Полученный шифротекст называется шифром подстановки.

uz – ўрнига қўйиш
en – substitution

2.11.15 **секретный ключ:** Ключ, который предназначен для использования при шифровании и дешифровании ограниченным числом корреспондентов.

uz – махфий калит
en – secret key

2.11.16 **симметричная криптография:** Криптография, в которой для шифрования и дешифрования используется один и тот же ключ.

uz – симметрик криптография
en – symmetric cryptography

2.11.17 **шифрование;** *кодирование*: Криптографическое преобразование данных.

Примечания

1 Результатом шифрования является шифротекст.

2 Обратный процесс называется дешифрование.

3 См. также криптография с открытым ключом, симметричная криптография, необратимое шифрование.

uz – шифрлаш, кодлаш
en – encryption, encipherment

2.11.18 **шифротекст:** Данные, получаемые в результате использования шифрования, семантическое содержимое которых не доступно без использования криптографических методов.

uz – шифрланган матн
en – ciphertext

2.12 Защита чувствительной информации

2.12.1 **антивирусная программа:** Программа, предназначенная для обнаружения вирусов и, возможно, предлагающая удалить или удаляющая их.

uz – вирусга қарши дастур
en – antivirus program

2.12.2 **аудит компьютерной системы:** Экспертиза процедур, используемых в системе обработки данных, для оценки их эффективности и правильности выполнения, а также выдача

uz – компьютер тизимининг аудити
en – computer-system audit

рекомендаций по повышению безопасности.

2.12.3 **аутентификация данных:** Процесс проверки целостности данных.

Примечание - Примером аутентификации данных является проверка того, что полученные данные идентичны отправленным данным, а также проверка того, что программа не заражена вирусом.

uz – маълумотларни аутентификация қилиш
en – data authentication

2.12.4 **биометрический:** Использующий для аутентификации личности ее определенные отличительные черты, которые являются уникальными персональными характеристиками, например, отпечатки пальцев, рисунок кровеносных сосудов глаза, тембр голоса.

uz – биометрик
en – biometric

2.12.5 **валидация:** Подтверждение посредством представления объективных свидетельств того, что требования, предназначенные для конкретного использования или применения, выполнены.

uz – валидация
en – validation

2.12.6 **верификация:** 1 Подтверждение посредством представления объективных свидетельств того, что установленные требования были выполнены.

Примечание – Верификацию также можно назвать тестированием на соответствие.

2 Процесс сравнения двух уровней спецификации средств вычислительной техники или автоматизированных систем на надлежащее соответствие.

uz – верификация
en – verification

2.12.7 **взаимное недоверие:** Отношения между взаимодействующими логическими объектами, когда ни один из них не полагается на безошибочность или надежность выполнения функций другим логическим объектом относительно некоторых свойств.

uz – ўзаро ишончсизлик
en – mutual suspicion

2.12.8 **журнал аудита:** Данные, собираемые для последующего использования при проведении аудита безопасности.

uz – аудит дафтари
en – audit trail

2.12.9 **защита приватности:** Реализация мер, гарантирующих сохранение личной тайны.

Примечание – К этим мерам относятся защита персональных данных и ограничения на их сбор, обобщение и обработку.

uz – норасмийликни муҳофаза қилиш
en – privacy protection

2.12.10 **использование ловушек:** Умышленная установка очевидных брешей в системе обработки данных, предназначенных для обнаружения попыток проникновения или введения в заблуждение нарушителя, когда он воспользуется этими брешами.

uz – қопқонлардан фойдаланиш
en – entrapment

2.12.11 **код аутентификации сообщений:** Последовательность битов, являющаяся функцией обоих данных (открытого текста или шифротекста) и секретного ключа, которая присоединяется к данным, чтобы обеспечить аутентификацию данных.

Примечание – Функция, используемая для генерации кода аутентификации сообщений, обычно является односторонней функцией.

uz – хабарларни аутентификация қилиш коди
en – message authentication code

2.12.12 **код обнаружения манипуляций;** *код обнаружения модификаций*: Последовательность битов, являющаяся функцией данных, к которым она добавлена, чтобы можно было обнаруживать наличие манипуляций.

Примечания

1 Полученное сообщение (данные плюс код обнаружения манипуляций) может быть зашифровано, чтобы обеспечить секретность или аутентификацию данных.

2 Функция, используемая для генерации кода обнаружения манипуляций, должна быть общедоступной.

uz – манипуляцияларни аниқлаш коди, модификацияларни аниқлаш коди
en – manipulation detection code, modification detection code

2.12.13 **контрмера:** Действие, устройство, процедура, метод или другая мера, которая предназначена для сведения к минимуму уязвимости.

uz – қарши чора
en – countermeasure

2.12.14 **контроль нажатия клавиш:** Определение правильности ввода данных с помощью метода повторного ввода тех же самых данных с клавиатуры.

uz – клавишлар босилишини назорат қилиш
en – keystroke verification

STANDARTLASHTIRISH ... INSTITUTI
MAZKUR HUJJATNING ... NUSXASI
AXBOROT TEXNOLOGIYALARI ... BO'LIMI
TOSHKENT ETIKSH ... KUTUBXONASI

2.12.15 **непризнание участия:** Отрицание одним из логических объектов, участвующих в обмене данными, полного или частичного своего участия в этом обмене.

uz – иштирокни тан олмаслик
en – repudiation

2.12.16 **нотаризация:** Регистрация данных доверенной третьей стороной, которая обеспечит впоследствии подтверждение таких их характеристик, как содержимое, отправитель, время и получатель.

uz – нотариаллаштириш
en – notarization

2.12.17 **обнаружение манипуляций;** *обнаружение модификаций*: Процедура, которая используется для обнаружения случайных или умышленных модификаций данных.

uz – манипуляцияларни аниқлаш, модификацияларни аниқлаш
en – manipulation detection, modification detection

2.12.18 **обратный вызов;** *обратный набор*: Процедура, используемая для аутентификации вызывающего терминала следующим образом: вначале система обработки данных идентифицирует вызывающий терминал, далее происходит разъединение вызова, а затем набирается номер вызывающего терминала.

uz – қайта чақириш, қайта рақам териш
en – call-back, dial-back

2.12.19 **остаточные данные:** Данные, оставшиеся на носителе данных после удаления всего файла или его части.

Примечание – Остаточные данные могут быть восстановлены, пока не будет выполнена очистка носителя данных.

uz – қолдиқ маълумотлар
en – residual data

2.12.20 **отказоустойчивый:** Предотвращающий компрометацию в случае отказа.

uz – бузилишларга барқарор
en – failsafe

2.12.21 **очистка:** Перезапись категорированных данных на носитель данных, имеющий определенный гриф секретности и категорию защиты, для того, чтобы этот носитель данных можно было неоднократно использовать для записи данных, имеющих тот же самый гриф секретности и категорию защиты.

uz – тозалаш
en – clearing

2.12.22 **понижение категории безопасности:** Удаление чувствительной информации из документа для уменьшения его чувствительности.

uz – хавфсизлик категориясини пасайтириш
en – sanitizing

2.12.23 **порядок действий в чрезвычайных ситуациях:** Альтернативный нормальному течению процесса порядок действий, который выполняется при возникновении нештатной, но предполагаемой ситуации.

uz – фавқулодда вазиятларда ҳаракат қилиш тартиби
en – contingency procedure

2.12.24 **проверка достоверности данных:** Процесс, используемый для определения точности данных, их полноты или соответствия заданным критериям.

Примечание - Проверка достоверности данных может включать проверки их форматов и полноты, контрольные тесты ключа, проверки корректности и ограничений.

uz – маълумотларнинг ишончлилигини текшириш
en – data validation

2.12.25 **разграничение обязанностей:** Разделение ответственности в отношении чувствительной информации таким образом, чтобы действующее в одиночку лицо, могло скомпрометировать безопасность только ограниченной части системы обработки данных.

uz – мажбуриятларни белгилаш
en – separation of duties

2.12.26 **сигнатура вируса:** Уникальная последовательность битов, которая присуща каждой копии специфического вируса и которая может быть использована сканирующей программой для обнаружения его присутствия.

uz – вирус сигнатураси
en – virus signature

2.12.27 **средство защиты:** Функциональный блок, используемый в качестве фильтра безопасности между двумя системами обработки данных, имеющими разные уровни безопасности, или между терминалом пользователя и базой данных, и предназначенный для отфильтровывания данных, для доступа к которым у пользователя отсутствуют полномочия.

uz – муҳофаза қилиш воситаси
en – guard, security tool

2.12.28 **тестирование на проникновение:** Исследование функций системы обработки данных с целью поиска способов обхода компьютерной безопасности.

uz – суқулиб кириш имкониятини тестлаш
en – penetration testing

O'ZSTANDART
STANDARTLASHTIRISH
MILLIY
AXBOROT

2.12.29 **фильтр безопасности:** Доверенная компьютерная система, которая реализует политику безопасности для данных, циркулирующих в системе.

uz – хавфсизлик фильтри
en – security filter

2.12.30 **цифровая подпись:** Данные, добавляемые к сообщению и позволяющие получателю сообщения проверять подлинность отправителя.

uz – рақамли имзо
en – digital signature

2.12.31 **цифровой конверт:** Данные, добавляемые к сообщению и позволяющие предполагаемому получателю проверять целостность содержания сообщения.

uz – рақамли конверт
en – digital envelope

2.13 Средства защиты информации

2.13.1 **антивирусное программное обеспечение:** Специальное программное обеспечение, предназначенное для выявления и деактивации (блокирования) вредоносного программного кода, специально созданного для нарушения целостности, доступности и конфиденциальности данных.

uz – антивирусли дастурий таъминот
en – antivirus software

2.13.2 **аппаратное средство защиты информации:** Специальное защитное устройство или приспособление, входящее в комплект технического средства обработки информации.

uz – ахборотни муҳофаза қилишнинг аппарат воситаси
en – information security hardware

2.13.3 **законодательные средства защиты информации:** Законодательные акты страны, которые регламентируют правила использования, обработки и передачи информации ограниченного доступа и устанавливают меры ответственности за нарушение этих правил.

uz – ахборотни муҳофаза қилишнинг қонунлаштирилган воситалари
en – legal protection means

2.13.4 **комплекс средств защиты;** КСЗ: Совокупность аппаратных, программных или аппаратно-программных средств, создаваемая и поддерживаемая для обеспечения защиты средств вычислительной техники или автоматизированных систем от несанкционированного доступа к информации.

uz – муҳофаза қилиш воситаларикомплекси; МВК
en – trusted computing base; TCB

2.13.5 **межсетевой экран:** Локальное (однокомпонентное) или функционально-распреде-ленное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в систему и/или выходящей из системы.

Примечания

1 Межсетевой экран обеспечивает защиту системы посредством фильтрации информации, т.е. анализа по совокупности критериев и принятия решения о ее распространении в (из) систему(ы) на основе заданных правил, проводя таким образом разграничение доступа субъектов из одной системы к объектам другой системы.

2 Средство защиты, устанавливаемое на стыке двух сетей, защищающее одну сеть от трафика, циркулирующего в другой сети, и служащее для предотвращения атак извне.

uz – тармоқлараро экран
en – firewall

2.13.6 **многоуровневое устройство:** Функциональный блок, который может одновременно обрабатывать данные двух или более уровней безопасности без риска нарушения компьютерной безопасности.

uz – кўп даражали қурилма
en – multilevel device

2.13.7 **морально-этические средства защиты информации:** Всевозможные нормы, сложившиеся традиционно в государстве и обществе. Эти нормы большей частью не являются обязательными, как законодательные меры, однако, несоблюдение их ведет обычно к потере авторитета и престижа человека.

uz – ахборотни муҳофаза қилишнинг маънавий-аҳлоқий воситалари
en – moral and ethical protection means

2.13.8 **одноуровневое устройство:** Функциональный блок, который может обрабатывать в данное время данные только одного уровня безопасности.

uz – бир даражали қурилма
en – single-level device

2.13.9 **организационные средства защиты информации:** Организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации сети телекоммуникаций для обеспечения защиты информации.

Примечание - Организационные мероприятия охватывают все структурные элементы сети на всех этапах их жизненного цикла (проектирование, испытание и эксплуатация).

uz – ахборотни муҳофаза қилишнинг ташкилий воситалари
en – organizational protection means

O'ZSTANDART
MILLIY ETALON

2.13.10 **программное средство защиты информации:** Специальная программа, входящая в комплект программного обеспечения и предназначенная для защиты информации.

uz – ахборотни муҳофаза қилишнинг дастурий воситаси
en – information security software

2.13.11 **система защиты информации [данных]:** Комплекс аппаратных, программных и криптографических средств, а также мероприятий, обеспечивающих защиту информации (данных) от случайного или преднамеренного разрушения, искажения или использования.

uz – ахборот [маълумотлар]ни муҳофаза қилиш тизими
en – information [data] protection system

2.13.12 **средства защиты информации;** СЗИ: Технические, криптографические, программные и другие средства, предназначенные для защиты информации, средств, в которых они реализованы, а также средства контроля эффективности защиты информации.

uz – ахборотни муҳофаза қилиш воситалари; АМВ
en – protection facilities of information

2.13.13 **средства защиты информации от несанкционированного доступа:** Аппаратные, программные, аппаратно-программные, криптографические средства, предназначенные для предотвращения или существенного затруднения несанкционированного доступа, а также средства контроля эффективности защиты информации.

uz – ахборотни рухсатсиз фойдалана олишдан муҳофаза қилиш воситалари
en – protection facilities of information from unauthorized access

2.13.14 **средства имитозащиты:** Аппаратные, программные и аппаратно-программные средства, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации.

uz – имитомуҳофаза воситалари
en – imitoprotection means

2.13.15 **средства кодирования:** Средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций.

uz – кодлаш воситалари
en – coding tools

2.13.16 **средства технической защиты информации:** Аппаратные, программные или аппаратно-программные средства, обеспечивающие техническую защиту информации на стадиях ее формирования, передачи, приема, преобразования, отображения и хранения.

uz – ахборотни техник мухофаза қилиш воситаси
en – facilities of technical protection of information

2.13.17 **средства шифрования:** Аппаратные, программные или 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.

uz – шифрлаш воситалари
en – facilities of cryptooperation

2.13.18 **средства электронной цифровой подписи:** Совокупность технических и программных средств, обеспечивающих создание электронной цифровой подписи в электронном документе, подтверждение подлинности электронной цифровой подписи, создание открытых и закрытых ключей электронной цифровой подписи.

uz – электрон рақамли имзо воситалари
en – facilities of electronic digital signature

2.13.19 **средство криптографической защиты информации:** Аппаратные, программные или аппаратно-программные средства, осуществляющие криптографические преобразования информации для обеспечения ее безопасности.

Примечание – К средствам криптографической защиты информации относятся также средства изготовления ключевых документов и сами ключевые документы (независимо от вида носителя ключевой информации).

uz – ахборотни криптографик муҳофаза қилиш воситаси
en – cryptographic information protection facility

2.13.20 **технические [аппаратно-программные] средства защиты информации:** Различные электронные устройства и специальные программы, которые выполняют самостоятельно или в комплексе с другими средствами функции защиты информации, например, идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий.

uz – ахборотни муҳофаза қилишнинг техник [аппарат-дастурий] воситалари
en – technical [hardware and software] protection means

2.13.21 **физическая защита:** Механизмы и процедуры, предназначенные для защиты компонентов телекоммуникационной или информационной систем и их структуры от физического ущерба, возникающего вследствие умышленных действий злоумышленников или халатности обслуживающего персонала.

uz – жисмоний муҳофаза қилиш
en – physical protection

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, METROLOGIYA
VA SERTIFIKATLASHTIRISH MARKAZI
AXBOROT TARQATISH BO'LIMI

2.13.22 **физические средства защиты:** Автономные устройства и системы, специально предназначенные для создания физических препятствий на возможных путях проникновения и доступа злоумышленника.

Примечание – Физическими средствами защиты могут быть замки на дверях, где размещена аппаратура, решетки на окнах, электронно-механическое оборудование охранной сигнализации.

uz – жисмоний муҳофаза қилиш воситалари
en – physical protection means

2.14 Информационная безопасность сетей телекоммуникаций

2.14.1 **администратор [руководящий орган] системы обеспечения информационной безопасности сети телекоммуникаций:** Субъект инфокоммуникационной структуры сети телекоммуникаций, ответственный за выполнение процессов обеспечения информационной безопасности в сети телекоммуникаций.

uz – телекоммуникациялар тармоғи ахборот хавфсизлигини таъминлаш тизимининг маъмури [раҳбарий орган]
en – administrator [governing body] of system of information security of telecommunication network

2.14.2 **архитектура системы обеспечения информационной безопасности сети телекоммуникаций:** Совокупность органов, служб и средств системы обеспечения информационной безопасности сети телекоммуникаций, объектов информационной безопасности сети, а также процессов взаимодействия этих объектов между собой и с подсистемой управления системы обеспечения информационной безопасности сети телекоммуникаций.

uz – телекоммуникациялар тармоғи ахборот хавфсизлигини таъминлаш тизимининг архитектураси
en – architecture of system of information security of telecommunication network

2.14.3 **базовый уровень информационной безопасности сети телекоммуникаций:** Установленный нормативными документами минимальный набор требований информационной безопасности, обеспечиваемый введенными в систему обеспечения информационной безопасности сети телекоммуникаций средствами защиты информации.

uz – телекоммуникациялар тармоғи ахборот хавфсизлигининг таянч даражаси
en – base level of information security of telecommunication network

O'ZBEKISTON STANDARTLASHTIRISH MILLIY AXBOROT TEXNIK JONIY ETISH

2.14.4 **безопасность сети телекоммуникаций:** Способность сети телекоммуникаций противодействовать определенному множеству угроз, преднамеренных или непреднамеренных дестабилизирующих воздействий на входящие в состав сети средства, линии телекоммуникаций и технологические процессы (протоколы), которые могут привести к ухудшению качества услуг, предоставляемых сетью телекоммуникаций.

uz – телекоммуникациялар тармоғининг хавфсизлиги
en – security of telecommunication network

2.14.5 **воздействие [атака] нарушителя на сеть телекоммуникаций:** Совокупность действий (операций) нарушителя информационной безопасности, направленная на реализацию угрозы информационной безопасности сети телекоммуникаций.

uz – бузғунчининг телекоммуникациялар тармоғига таъсири [ҳужуми]
en – action [attack] of intruder on telecommunication network

2.14.6 **доступность [готовность] информационной сферы сети телекоммуникаций:** Способность сети телекоммуникаций обеспечить пользователям согласованные условия доступа к предоставляемым услугам телекоммуникаций и их получение, в том числе и в условиях возможных воздействий нарушителя информационной безопасности на информационную сферу сети телекоммуникаций.

uz – телекоммуникациялар тармоғи ахборот соҳасидан фойдалана олишлик [тайёрлиги]
en – availability of information sphere of telecommunication network

2.14.7 **защищенная сеть телекоммуникаций:** Сеть телекоммуникаций, обеспечивающая заданный уровень информационной безопасности по отношению к заданному множеству угроз информационной безопасности и заданный набор услуг информационной безопасности.

uz – муҳофаза қилинган телекоммуникациялар тармоғи
en – protected telecommunication network

2.14.8 **защищенность информационной сферы сети телекоммуникаций:** Способность сети телекоммуникаций к предотвращению, либо обнаружению и своевременной ликвидации последствий воздействия нарушителя информационной безопасности на ее информационную сферу.

uz – телекоммуникациялар тармоғи ахборот соҳасининг муҳофаза қилинганлиги
en – protection of information sphere of telecommunication network

2.14.9 **информационная безопасность сети телекоммуникаций:** Способность сети телекоммуникаций противостоять преднамеренным и непреднамеренным дестабилизирующим воздействиям (угрозам безопасности) на входящие в состав сети средства и линии телекоммуникаций в процессе приема и передачи, обработки и хранения информации, которые могут привести к снижению заданного уровня качества услуг, предоставляемых сетью телекоммуникаций, или к ухудшению заданных качественных характеристик работы сети и, тем самым, к нанесению ущерба ее владельцам или пользователям.

uz – телекоммуникациялар тармоғининг ахборот хавфсизлиги
en – information security of telecommunication network

2.14.10 **информационная инфраструктура сети телекоммуникаций:** Совокупность центров хранения, обработки и передачи информации, каналов информационного обмена, линий телекоммуникаций, систем и средств обеспечения информационной безопасности сети телекоммуникаций.

uz – телекоммуникациялар тармоғининг ахборот инфраструктураси
en – information infrastructure of telecommunication network

2.14.11 **информационная сфера сети телекоммуникаций:** Совокупность информационных ресурсов и информационной инфраструктуры сети телекоммуникаций.

uz – телекоммуникациялар тармоғининг ахборот соҳаси
en – information sphere of telecommunication network

2.14.12 **информационные ресурсы сети телекоммуникаций:** Совокупность хранимых (используемых для обеспечения процессов функционирования), обрабатываемых и передаваемых данных, содержащих информацию пользователей или системы управления сети телекоммуникаций.

uz – телекоммуникациялар тармоғининг ахборот ресурслари
en – information resources of telecommunication network

2.14.13 **качество обслуживания сети телекоммуникаций в условиях возможных воздействий нарушителя:** Гарантируемая совокупность измеряемых и регулируемых средствами сети телекоммуникаций ее качественных характеристик функционирования, характеризующая заданный (согласованный) уровень защищенности информационной сферы сети телекоммуникаций.

uz – бузғунчининг эҳтимолий таъсирлари шароитларида телекоммуникациялар тармоғига хизмат кўрсатиш сифати
en – quality of service of telecommunication net-

work in condition of possible action of intruder

2.14.14 **качество службы информационной безопасности сети телекоммуникаций:** Совокупность определяемых, измеряемых и регулируемых параметров предотвращения, обнаружения и ликвидации угрозы информационной безопасности, противодействие которой является задачей данной службы информационной безопасности сети телекоммуникаций.

uz – телекоммуникациялар тармоғи ахборот хавфсизлиги хизматининг сифати
en – quality of service of information security of telecommunication network

2.14.15 **конфиденциальность информационной сферы сети телекоммуникаций:** Способность сети телекоммуникаций обеспечить сохранность подлежащей защите информации, ее информационной сферы от несанкционированного ознакомления.

uz – телекоммуникациялар тармоғи ахборот соҳасининг конфиденциаллиги
en – confidentiality of information sphere of telecommunication network

2.14.16 **меры обеспечения информационной безопасности сети телекоммуникаций:** Набор функций, определяющих возможности механизмов обеспечения информационной безопасности сети телекоммуникаций по непосредственной или косвенной реализации требований по безопасности информации.

uz – телекоммуникациялар тармоғининг ахборот хавфсизлигини таъминлаш чоралари
en – measures of information security of telecommunication network

2.14.17 **механизм обеспечения информационной безопасности сети телекоммуникаций:** Аппаратно-программные и организационные средства системы обеспечения информационной безопасности сети телекоммуникаций, реализующие в соответствии с заданной политикой информационной безопасности сети один или несколько аспектов защиты от угроз информационной безопасности сети в соответствии с одним из трех, перекрывающих друг друга классов защиты: предотвращения, обнаружения и ликвидации последствия воздействия нарушителя информационной безопасности сети телекоммуникаций.

Примечание – К механизмам обеспечения информационной безопасности сети телекоммуникаций относятся: механизм контроля доступа, механизм аутентификации сообщений, механизм обменной аутентификации.

uz – телекоммуникациялар тармоғининг ахборот хавфсизлигини таъминлаш механизми
en – mechanism of information security of telecommunication network

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH DAVLAT
MILLIY FONDI KUTUBXONASI
AXBOROT TEXNOLOGIYALARI

2.14.18 **мониторинг системы обеспечения информационной безопасности сети телекоммуникаций:** Получение и анализ информации о состоянии ресурсов системы обеспечения информационной безопасности сети телекоммуникаций с помощью специальных средств контроля в реальном масштабе времени.

uz – телекоммуникациялар тармоғи ахборот хавфсизлигини таъминлаш тизимининг мониторинги
en – monitoring system of information security of telecommunication network

2.14.19 **мониторинг событий информационной безопасности сети телекоммуникаций:** Постоянный контроль и действия по наблюдению, получению, хранению, распознаванию и анализу информации, связанной с событиями информационной безопасности, выявлению фактов, признаков и причин нарушения установленных требований и объектов/субъектов, с которыми связаны эти нарушения.

uz – телекоммуникациялар тармоғи ахборот хавфсизлиги ҳодисаларининг мониторинги
en – monitoring events of information security of telecommunication network

2.14.20 **нарушитель информационной безопасности сети телекоммуникаций:** Физическое или юридическое лицо, техническое устройство или программа, процесс или событие, субъект или пользователь сети телекоммуникаций, производящие несанкционированные или непреднамеренные действия (операции) над ее информационной сферой, способные привести к потере одной или более характеристик информационной безопасности сети телекоммуникаций: конфиденциальности, целостности, доступности и подотчетности информационной сферы.

uz – телекоммуникациялар тармоғи ахборот хавфсизлигининг бузғунчиси
en – intruder of information security of telecommunication network

2.14.21 **несанкционированный доступ к сети телекоммуникаций:** Доступ к аппаратно-программному обеспечению и циркулирующим в сети данным пользователя и данным управления сетью без санкции ответственных лиц с целью незаконного использования ресурсов или несанкционированного воздействия на объекты сети (в том числе и информацию управления сетью) или передаваемые через них данные для дезорганизации процесса передачи данных (например, его блокирования).

uz – телекоммуникациялар тармоғидан рухсатсиз фойдалана олиш
en – unauthorized access to telecommunication network

O'ZSTANDART
STANDARTLASHTIRISH
NAZORATINI
AXBOROT
JORIY ETISH

2.14.22 **объект информационной безопасности сети телекоммуникаций:** Объект сети телекоммуникаций, воздействия злоумышленника на который может привести к реализации угрозы информационной безопасности сети телекоммуникаций.

uz – телекоммуникациялар тармоғининг ахборот хавфсизлиги объекти
en – object of information security of telecommunication network

2.14.23 **подотчетность информационной сферы сети телекоммуникаций:** Свойство, позволяющее однозначно определять действия, способные привести к нарушению процесса обеспечения информационной безопасности какого-либо объекта относительно другого объекта.

uz – телекоммуникациялар тармоғи ахборот соҳасининг ҳисоб беришлиги
en – accountability of information sphere of telecommunication network

2.14.24 **политика информационной безопасности сети телекоммуникаций:** Совокупность требований и правил для объекта (объектов) информационной безопасности сети телекоммуникаций, разработанных оператором сети в целях противодействия определенным угрозам информационной безопасности сети с учетом ценности защищаемых ресурсов и стоимости системы обеспечения информационной безопасности сети телекоммуникаций.

uz – телекоммуникациялар тармоғининг ахборот хавфсизлиги сиёсати
en – policy of information security of telecommunication network

2.14.25 **риск информационной безопасности сети телекоммуникаций:** Значение вероятности и величина (характер) возможного ущерба пользователя, оператора связи или государства, полученного вследствие реализации нарушителем угрозы информационной безопасности сети телекоммуникаций.

uz – телекоммуникациялар тармоғининг ахборот хавфсизлиги риски (эҳтимолий хавфи)
en – risk of information security of telecommunication network

2.14.26 **система обеспечения информационной безопасности сети телекоммуникаций:** Совокупность правовых, организационных и технических мероприятий, служб и механизмов обеспечения информационной безопасности, норм, органов управления и исполнителей в определенной сети телекоммуникаций, направленных на обеспечение ее информационной безопасности.

uz – телекоммуникациялар тармоғининг ахборот хавфсизлигини таъминлаш тизими
en – system of information security of telecommunication network

2.14.27 **служба информационной безопасности сети телекоммуникаций:** Организационно-техническая структура оператора сети телекоммуникаций, реализующая политику безопасности этого оператора и обеспечивающая функционирование системы обеспечения безопасности сети телекоммуникаций.

uz – телекоммуникациялар тармоғининг ахборот хавфсизлиги хизмати
en – service of information security of telecommunication network

2.14.28 **субъект информационной безопасности сети телекоммуникаций:** Лицо или инициируемые от его имени процессы по выполнению действий над объектами информационной безопасности сети телекоммуникаций.

uz – телекоммуникациялар тармоғининг ахборот хавфсизлиги субъекти
en – subject of information security of telecommunication network

2.14.29 **телефонный пират;** *фрикер*: Злоумышленник, скрытно подключающийся с помощью различных устройств и приемов к телефонным сетям, например, с целью сделать бесплатные международные и междугородние звонки или скрыть свое местонахождение при проведении несанкционированных действий в сети Интернет, или оказать психологическое воздействие на конечного абонента.

uz – телефон қароқчиси, фрикер
en – phreaker

2.14.30 **технологическая безопасность сети телекоммуникаций:** Свойство аппаратно-программного обеспечения сети телекоммуникаций не иметь злоумышленных дефектов диверсионного типа, т.е. средств, способных по истечении определенного времени или по команде извне произвести действия, приводящие к нежелательным последствиям.

uz – телекоммуникациялар тармоғининг технологик хавфсизлиги
en – technological security of telecommunication network

2.14.31 **угроза информационной безопасности сети телекоммуникаций:** Предполагаемое воздействие злоумышленника на сеть телекоммуникаций, не предотвращение, не обнаружение и не ликвидация которого средствами сети может привести к снижению заданного уровня обеспечения информационной безопасности сети телекоммуникаций.

uz – телекоммуникациялар тармоғининг ахборот хавфсизлигига таҳдид
en – threat of information security of telecommunication network

Примечание - Результаты анализа последствий воздействия нарушителя с точки зрения риска информационной безопасности сети телекоммуникаций, к которо-

O‘ZSTANDART
STANDARTLASHTIRISH
NAZORATI MARKAZI
AXBOROT
JORIY ETILDI

му эти последствия могут привести, являются основой для составления списка наиболее опасных угроз информационной безопасности для данной сети телекоммуникаций.

2.14.32 **уровень информационной безопасности сети телекоммуникаций:** Совокупность требований информационной безопасности сети телекоммуникаций, обеспечиваемых введенными в сеть телекоммуникаций средствами защиты информации.

uz – телекоммуникациялар тармоғининг ахборот хавфсизлиги даражаси
en – level of information security of telecommunications network

2.14.33 **устойчивость функционирования сети телекоммуникаций:** Способность сети телекоммуникаций выполнять свои функции при выходе из строя части элементов сети в результате воздействия дестабилизирующих факторов.

uz – телекоммуникациялар тармоғи ишлашининг барқарорлиги
en – stability of functioning of telecommunication network

2.14.34 **уязвимость сети телекоммуникаций:** Недостатки технологии процесса передачи данных и управления, средств телекоммуникаций, мер и средств обеспечения информационной безопасности сети телекоммуникаций, позволяющие нарушителю совершать действия, приводящие к успешной реализации угрозы информационной безопасности сети телекоммуникаций.

uz – телекоммуникациялар тармоғининг заифлиги
en – vulnerability of telecommunication network

2.14.35 **целостность информационной сферы сети телекоммуникаций:** Способность сети телекоммуникаций предотвращать несанкционированное изменение ее информационной сферы или обеспечивать своевременное восстановление процесса функционирования, нарушенного вследствие непредотвращенного воздействия нарушителя информационной безопасности сети телекоммуникаций на ее информационную сферу.

uz – телекоммуникациялар тармоғи ахборот соҳасининг яхлитлиги
en – integrity of information sphere of telecommunication network

2.14.36 **цель обеспечения информационной безопасности сети телекоммуникаций:** Сформулированное намерение противостоять заданным угрозам информационной безопасности сети телекоммуникаций и/или удовлетворять заданной политике информационной безопасности сети телекоммуникаций.

uz – телекоммуникациялар тармоғининг ахборот хавфсизлигини таъминлаш мақсади
en – objective of provision of information security of telecommuni-cation network

STANDARTLASHTIRISH DAVLAT
MUASSASASI KUTUBXONASI
AXBOROT TEXNOLOGIYALARI
JORIY ETISH BO'LIMI

2.14.37 **эксплуатационная безопасность сети телекоммуникаций:** Защищенность процесса функционирования сети телекоммуникаций от угроз несанкционированного доступа нарушителей к объектам сети и информации управления и к данным, циркулирующим в ней, с целью ознакомления с передаваемой информацией управления сетью, а также преднамеренного воздействия на объекты, информацию управления сетью и передаваемые данные для дезорганизации функционирования сети телекоммуникаций.

uz – телекоммуникация лар тармоғидан фойдаланиш хавфсизлиги
en – maintenance security of telecommunication network

2.15 Информационная безопасность мобильной связи

2.15.1 **международный идентификатор абонента:** Уникальный специализированный код для регистрации абонента в сети мобильной связи стандарта GSM, хранимый в SIM-карте и имеющий следующий формат:

a) трехразрядный мобильный код страны;
b) двухразрядный мобильный код сети;
c) десятиразрядный код абонента.

uz – абонентнинг халқаро идентификатори
en – international mobile subscriber identity

2.15.2 **мобильный код сети:** Индекс из двух цифр в заголовке международного идентификатора абонента, определяющий сеть, в которой абонент получил постоянную регистрацию.

uz – тармоқнинг мобил коди
en – mobile network code

2.15.3 **мобильный код страны:** Индекс из трех цифр в заголовке международного идентификатора абонента, определяющий код страны, где зарегистрирован абонент.

uz – мамлакатнинг мобил коди
en – mobile country code

2.15.4 **модуль идентификации абонента;** *SIM-карта*: Миниатюрная пластиковая карта с интегрированным кремниевым чипом, на котором записана информация о конкретном абоненте мобильной связи, необходимая для его идентификации в сети.

uz – абонентни идентификация қилиш модули; SIM-карта
en – subscriber identification module; SIM-card

2.15.5 **персональный идентификационный номер;** *ПИН-код*: Уникальный персональный код, хранимый в SIM-карте и используемый для аутентификации личности абонента.

uz – идентификацион шахсий рақам; ИШР-код
en – personal identification number; PIN

2.15.6 **персональный ключ разблокировки:** Ключ, используемый для разблокировки SIM-карты и служащий для ее защиты от несанкционированного использования.

uz – блокировкадан чиқаришнинг шахсий калити
en – personal unblocking key

2.15.7 **сменный модуль идентификации абонента:** Разновидность SIM-карты для сети мобильной связи третьего поколения стандарта CDMA2000, которая может быть легко переставлена из одного мобильного телефона в другой.

uz – абонентни идентификация қилишнинг алмаштириладиган модули
en – removable user identity module

2.15.8 **универсальный модуль идентификации абонента:** Универсальная SIM-карта в сети UMTS, аналогичная SIM-карте в GSM, но с более широким набором услуг.

uz – абонентни идентификация қилишнинг универсал модули
en – universal subscriber identification module

2.16 Режим секретности

2.16.1 **военная тайна:** Сведения военного характера, разглашение которых может повлечь тяжкие последствия для обороноспособности, государственной безопасности и Вооруженных Сил Республики Узбекистан.

uz – ҳарбий сир
en – military secret

2.16.2 **государственная тайна:** Сведения, разглашение которых может оказать отрицательное воздействие на качественное состояние военно-экономического потенциала республики или повлечь другие тяжкие последствия для обороноспособности, государственной безопасности, экономических и политических интересов Республики Узбекистан.

uz – давлат сири
en – state secret

2.16.3 **государственные секреты:** Особой важности, совершенно секретные и секретные военные, политические, экономические, научно-технические и иные сведения, охраняемые государством и ограничиваемые специальными перечнями.

uz – давлат сирлари
en – state secrets

Примечание - Государственные секреты Республики Узбекистан подразделяются на государственную, военную и служебную тайну.

O'ZSTANDART AGENTLIGI
STANDART
AXBOROT

2.16.4 **гриф секретности:** Реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и/или в сопроводительной документации на него.

Примечание – Грифом секретности на документе являются надпись, штамп и др., например, «совершенно секретно», «секретно», «для служебного пользования».

uz – махфийлик грифи
en – degree of classification

2.16.5 **допуск к государственным секретам:** Процедура оформления права гражданам Республики Узбекистан на доступ к сведениям, составляющим государственные секреты Республики Узбекистан, а уполномоченным органам - на проведение работ с использованием такой информации.

uz – давлат сирларидан фойдаланиш ҳуқуқи
en – access to state secret

2.16.6 **доступ к сведениям, составляющим государственные секреты:** Санкционированное полномочным должностным лицом фактическое ознакомление конкретного лица со сведениями, составляющими государственные секреты.

uz – давлат сирларини ташкил этувчи маълумотлардан фойдалана олиш
en – access to state secret information

2.16.7 **засекречивание сведений и их носителей:** Введение в предусмотренном законодательством Республики Узбекистан порядке для сведений, составляющих государственные секреты, ограничений на их распространение и на доступ к их носителям.

uz – маълумотлар ва уларни ташувчиларини махфийлаштириш
en – classification of information and its bearers as secret

2.16.8 **защищаемые помещения;** ЗП: Помещения (служебные помещения, актовые, конференц-залы и т.д.), специально предназначенные для проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций, переговоров и т.п.).

uz – муҳофаза қилинадиган хоналар; МХ
en – protectable rooms

2.16.9 **коммерческая тайна:** Информация, имеющая коммерческую ценность в научно-технической, технологической, производственной, финансово-экономической и других сферах в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и собственник этой информации принимает меры по защите ее конфиденциальности.

uz – тижорат сири
en – trade secret

O'ZSTANDART ... STANDARTLASHTIRISH ... AXBOROT ...

2.16.10 **контролируемая зона:** Пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание посторонних лиц и транспортных средств, не имеющих постоянного или разового допуска.

Примечание - Границами контролируемой зоны могут быть:

- периметр контролируемой территории организации;

- ограждающие конструкции охраняемого здания или охраняемой части здания, если оно размещено на неохраняемой территории.

uz – назорат килинадиган зона
en – controlled zone

2.16.11 **несанкционированный доступ к секретной информации:** Получение секретных сведений лицами, не имеющими права доступа к этим сведениям.

uz – махфий ахборотдан рухсат этилмаган тарзда фойдалана олиш
en – unauthorized access to secret information

2.16.12 **носители сведений, составляющих государственные секреты:** Физические лица и материальные объекты, в том числе физические поля, в которых сведения, составляющие государственные секреты, отражаются в виде памяти, символов, образов, сигналов, технических решений и процессов.

uz – давлат сирларини ташкил этувчи маълумотларни ташувчилар
en – bearers of state secrets

2.16.13 **перечень сведений, подлежащих засекречиванию в Республике Узбекистан:** Документ, утвержденный в установленном порядке, определяющий степень секретности сведений, разглашение или утрата которых причиняет либо может причинить ущерб государственным интересам Республики Узбекистан.

uz – Ўзбекистон Республикасида махфийлаштирилиши лозим бўлган маълумотлар рўйхати
en – list of information to be classified as secret in Republic of Uzbekistan

2.16.14 **разглашение секретных сведений:** Предание огласке или распространение с нарушением установленного порядка (правил) секретных сведений лицом, которому они были доверены или стали известны по службе или работе, в результате чего эти сведения стали достоянием посторонних лиц.

Примечания

1 К посторонним следует относить тех лиц, которым соответствующие сведения не были доверены и

uz – махфий маълумотларнинг ошкор этилиши
en – disclosure of secret information

не стали известны по службе или работе.

2 Разглашение может быть как устным (например, в ходе публичного выступления), так и письменным (опубликование в средствах массовой информации, сообщение в письме).

2.16.15 **разрушение секретной информации в средствах вычислительной техники:** Неправомерное или преднамеренное изменение, искажение или уничтожение секретной информации в результате неисправности технических средств, несовершенства и ошибок программного обеспечения, халатности обслуживающего персонала, стихийных бедствий или действий злоумышленников (нарушителей).

uz – ҳисоблаш техникаси воситаларида махфий ахборотнинг бузилиши
en – destruction of secret information in facilities of computing machinery

2.16.16 **рассекречивание сведений и их носителей:** Снятие ранее введенных в предусмотренном законодательством Республики Узбекистан порядке ограничений на распространение сведений, составляющих государственные секреты, и на доступ к их носителям.

uz – маълумотлар ва уларнинг ташувчиларини ошкор қилиш
en – declassification of information and its bearers as secret

2.16.17 **режим разграничения доступа:** Порядок доступа лиц к техническим средствам, программам и секретной информации при ее обработке на средствах вычислительной техники в соответствии с заранее разработанными и утвержденными правилами.

uz – фойдалана олишни чеклаш режими
en – access demarcation mode

2.16.18 **режим секретности:** Установленный нормативными актами высших органов государственной власти и управления единый порядок обеспечения сохранности государственных секретов, включающий в себя систему административно-правовых, организационных, инженерно-технических и иных мер.

uz – махфийлик режими
en – secrecy mode

2.16.19 **режимно-секретный орган:** Самостоятельное структурное подразделение, разрабатывающее и осуществляющее мероприятия по обеспечению режима секретности и проводящее постоянный контроль за его соблюдением в организациях, где ведутся секретные работы.

uz – махфий-режимли орган
en – organ of regime and secret

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH
MILLIY
AXBOROT
FONDI

2.16.20 **режимные объекты:** Военные и специальные объекты, воинские части, предприятия, организации, учреждения, для функционирования которых установлены дополнительные меры безопасности.

uz – режимли объектлар
en – secret objects

2.16.21 **сведения особой важности:** Наиболее охраняемые государством сведения из числа составляющих государственную тайну, распространение которых может оказать отрицательное воздействие на качественное состояние военно-экономического потенциала и безопасности государства или нанести серьёзный ущерб политическим интересам Республики Узбекистан.

uz – алоҳида аҳамиятга молик маълумотлар
en – highly important information

2.16.22 **секретная работа:** Научно-исследовательские и опытно-конструкторские, проектные, технологические, изыскательские, диссертационные, дипломные и иные работы, в процессе выполнения которых образуются сведения, составляющие государственные секреты, или секретные сведения.

uz – махфий иш
en – secret work

2.16.23 **секретные сведения:** Сведения, составляющие служебную и военную тайну.

uz – махфий маълумотлар
en – secret information

2.16.24 **служебная тайна:** Сведения в области науки, техники, производства и управления, разглашение которых может нанести ущерб интересам Республики Узбекистан.

uz – хизмат сири
en – official secret

2.16.25 **совершенно секретные сведения:** Сведения из числа составляющих государственную тайну за исключением сведений особой важности.

uz – мутлақо махфий маълумотлар
en – top secret information

2.16.26 **утечка секретной информации:** Неправомерный выход сведений, составляющих государственную и служебную тайну, за пределы организации или круга лиц, которым эти сведения доверены.

uz – махфий ахборотнинг чиқиб кетиши
en – secret information leaking

O‘ZBEKISTON STANDARTLARI AXBOROT MARKAZI

2.16.27 **утрата документов или изделий [предметов], содержащих секретные сведения:** Выход (в том числе и временный) документов или изделий из владений ответственного за их сохранность лица, которому они были доверены по службе или работе, являющийся результатом нарушения установленных правил обращения с ними, вследствие чего эти документы или изделия стали, либо могли стать достоянием посторонних лиц.

uz – махфий маълумотлар бўлган ҳужжатлар ёки буюмларнинг [нарсаларнинг] йўқолиши
en – loss of documents or products [units], containing secret information

2.17 Защита и восстановление данных

2.17.1 **архивирование:** Хранение резервных файлов и любых взаимосвязанных с ними журналов в течение заданного периода времени.

uz – архивлаш
en – archiving

2.17.2 **архивный файл:** Файл, сохраняемый для более позднего изучения или верификации, для безопасности или любой другой цели.

uz – архивга оид файл
en – archive file

2.17.3 **воссоздание данных:** Метод реставрации данных путем компоновки данных из частей доступных альтернативных источников.

uz – маълумотларни янгитдан яратиш
en – data reconstitution

2.17.4 **заархивированный файл:** Файл, для которого существует архивный файл.

uz – архивлаштирилган файл
en – archived file

2.17.5 **запасной пункт обработки данных;** *холодный резерв*: Возможно минимальное количество оборудования, необходимого для инсталяции и задействования резервной системы обработки данных.

uz – маълумотларни қайта ишлашнинг захира пункти; совуқ резерв
en – cold site; shell site

2.17.6 **защита файла:** Реализация соответствующих административных, технических или физических мер для предотвращения несанкционированного доступа, модификации или удаления файла.

uz – файлни муҳофаза қилиш
en – file protection

2.17.7 **обратное восстановление:** Использование более поздней версии и данных, записанных в журнал, для воссоздания более ранней версии данных.

uz – қайта тик-лаш
en – backward recovery

O‘ZSTANDART STANDARTLASHTIRISH MILLIY AXBOROT TIZIMI

2.17.8 **план действий при чрезвычайных ситуациях;** *план восстановления*: План, предусматривающий процедуры резервирования, действия при авариях и восстановление после стихийных бедствий.

uz – фавқулодда вазиятларда ҳаракат қилиш режаси; тиклаш режаси
en – contingency plan disaster; recovery plan

2.17.9 **процедура резервирования:** Процедура, предусматривающая реставрацию данных после сбоя или аварии.

Примечание – Примером процедуры резервирования является создание резервных файлов.

uz – резервлаш процедураси
en – backup procedure

2.17.10 **прямое восстановление:** Использование более ранней версии и данных, записанных в журнал, для воссоздания более поздней версии данных.

uz – бевосита тиклаш
en – forward recovery

2.17.11 **резервный пункт обработки данных;** *горячий резерв*: Полностью оборудованный вычислительный центр, который обеспечивает возможность немедленной альтернативной обработки данных.

uz – маълумотларни қайта ишлашнинг резерв пункти; иссиқ резерв
en – hot site; hot standby

2.17.12 **резервный файл:** Файл, создаваемый для возможно более поздней реставрации данных.

Примечание – Примером резервного файла является копия файла, сохраняемая в резервном пункте обработки данных.

uz – резерв файл
en – backup file

2.17.13 **реконструкция данных:** Метод реставрации данных путем анализа первоисточников.

uz – маълумотларни реконструкция қилиш
en – data reconstruction

2.17.14 **реставрация данных:** Восстановление потерянных или зараженных данных.

Примечание – Совокупность метода копирования архивных данных, метода реконструкции данных из исходных данных или метода воссоздания данных из альтернативных источников.

uz – маълумотларни реставрация қилиш
en – data restoration

O‘ZSTANDART
STANDARTLASHTIRISH
NAZORAT-D
AXBOROT
JORIY ET

2.18 Защита от копирования

2.18.1 **блокирование:** Использование специальных методов защиты данных или программного обеспечения от несанкционированного копирования.

uz – блокировка қилиш
en – padlocking

2.18.2 **выравнивание сектора:** Метод защиты от копирования, позволяющий при проверке правильности установки секторов от дорожки к дорожке определить, является ли диск несанкционированной копией или нет.

uz – секторни тўғрилаш
en – sector alignment

2.18.3 **дополнительная дорожка:** Часть метода защиты от копирования, когда на диск сверх стандартного количества дорожек записывается еще одна дорожка.

uz – қўшимча йўлка
en – extra track

2.18.4 **дополнительный сектор:** Часть метода защиты от копирования, когда на дорожку сверх стандартного количества секторов записывается еще один сектор.

uz – қўшимча сектор
en – extra sector

2.18.5 **защита от копирования:** Использование специальных методов для обнаружения или предотвращения несанкционированного копирования данных, программного или аппаратно-программного обеспечения.

uz – нусха кўчиришдан муҳофаза қилиш
en – copy protection

2.18.6 **контрольный [проверочный] код:** Машинные команды, которые читают часть диска, чтобы определить, не является ли он несанкционированной копией.

uz – назорат [текшириш] коди
en – checking code

2.18.7 **ложная разметка:** Способ защиты от копирования, при использовании которого на диске специально записываются дефектные секторы.

uz – чалғитувчи белги
en – bad sectoring

2.18.8 **ложный сектор:** Сектор, состоящий только из одного заголовка без данных, который многократно записывается на диск, чтобы его было невозможно скопировать с помощью программы несанкционированного копирования.

uz – чалғитувчи сектор
en – fake sector

O'ZBEKISTON STANDARTLASHTIRISH NAZORATINI AMALGA OSHIRUVCHI DAVLAT XIZMATI

2.18.9 **слабый бит:** Часть метода защиты от копирования, когда бит, специально записанный на диск при слабой напряженности магнитного поля, может интерпретироваться и как нуль, и как единица.

uz – суст бит
en – weak bit

2.18.10 **смещенная дорожка:** Часть метода защиты от копирования, когда дорожка на диск записывается в нестандартную позицию.

uz – силжиган йўлка
en – offset track

2.18.11 **спиральная дорожка:** Часть метода защиты от копирования, когда на диск записывается дорожка спиральной формы.

uz – спираль йўлка
en – spiral track

2.18.12 **суперсектор:** Часть метода защиты от копирования, когда на диск записывается сектор с размерами больше обычного.

uz – суперсектор
en – supersector

2.18.13 **широкая дорожка:** Часть метода защиты от копирования, когда в две или более смежных дорожек на диске записаны одни и те же данные.

uz – кенг йўлка
en – wide track

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH DEPARTAMENTI
NAZORAT N.L. [illegible]
AXBOROT [illegible]
JORIY ETISH [illegible]

3 Алфавитный указатель терминов на русском языке

Авторизация 2.9.1
Авторизованный субъект доступа 2.9.2
Агрегирование 2.6.1
Административная безопасность 2.1.1
Администратор безопасности 2.4.1
Администратор защиты 2.4.1
Администратор системы обеспечения информационной безопасности сети телекоммуникаций 2.14.1
Администрация системы защиты 2.4.2
Активная атака 2.8.1
Активная угроза 2.6.2
Активный перехват информации 2.6.3
Анализ рисков 2.7.1
Анализ трафика 2.6.4
Анализ угроз 2.6.5
Аналитическая атака 2.8.2
Антивирусная программа 2.12.1
Антивирусное программное обеспечение 2.13.1
Аппаратное средство защиты информации 2.13.2
Аппаратно-программные средства защиты информации . 2.13.20
Аппаратный токен 2.9.3
Архивирование 2.17.1
Архивный файл 2.17.2
Архитектура системы обеспечения информационной безопасности сети телекоммуникаций 2.14.2
Ассимметричная криптография 2.11.1
Атака 2.8.3
Атака нарушителя на сеть телекоммуникаций 2.14.5
Атака перебором открытого текста 2.8.4
Атака переполнения 2.8.5
Атака по известному открытому тексту 2.8.6
Атака полным перебором 2.8.7
Атака типа «отказ в обслуживании» 2.8.8
Атака только по шифротексту 2.8.9
Аттестация объектов информатизации 2.3.1
Аудит безопасности 2.4.3
Аудит компьютерной системы 2.12.2
Аутентификация 2.9.4
Аутентификация данных 2.12.3
Аутентификация личности 2.9.5
Аутентификация сообщения 2.9.6

O'ZBEKISTON STANDARTLASHTIRISH MILLIY AXBOROT TEXNOLOGIYALARI

Аутентичность 2.2.1
Базовый анализ рисков 2.7.2
Базовый уровень информационной безопасности сети телекоммуникаций 2.14.3
Безопасность 2.1.2
Безопасность данных 2.5.1
Безопасность информации 2.5.1
Безопасность связи 2.1.10
Безопасность сети телекоммуникаций 2.14.4
Биометрический 2.12.4
Блокирование 2.18.1
Блокирование передачи данных 2.6.6
Блокирование передачи информации 2.6.6
Брешь 2.6.7
Валидация 2.12.5
Верительные данные 2.9.7
Верификация 2.12.6
Взаимное недоверие 2.12.7
Вид доступа 2.9.8
Вирус 2.6.51
Внешний дестабилизирующий фактор 2.6.8
Внутреннее мошенничество 2.6.9
Внутренний дестабилизирующий фактор 2.6.10
Внутренняя атака 2.8.10
Военная тайна 2.16.1
Воздействие нарушителя на сеть телекоммуникаций 2.14.5
Воссоздание данных 2.17.3
Вредоносная программа 2.6.11
Временная бомба 2.6.12
Вход между строк 2.6.13
Выравнивание сектора 2.18.2
Горячий резерв 2.17.11
Государственная тайна 2.16.2
Государственные секреты 2.16.3
Готовность информационной сферы сети телекоммуникаций 2.14.6
Гриф секретности 2.16.4
Декодирование 2.11.2
Дестабилизирующее воздействие 2.6.14
Дестабилизирующий фактор 2.6.15
Дешифрование 2.11.2
Дискреционное управление доступом 2.9.9
Диспетчер доступа 2.9.10

O'ZSTANDART AGENTLIGI
STANDARTLARNI NAZORAT QILISH
AXBOROT TIZIMI
JORIY ETILGAN

Доверенная компьютерная система 2.1.3
Документ 2.5.2
Документированная информация 2.5.2
Домен безопасности 2.10.1
Дополнительная дорожка 2.18.3
Дополнительный сектор 2.18.4
Допуск 2.9.22
Допуск к государственным секретам 2.16.5
Достоверность 2.2.2
Доступ 2.9.11
Доступ к информации 2.9.12
Доступ к информационному ресурсу 2.9.13
Доступ к сведениям, составляющим государственные секреты 2.16.6
Доступ на запись 2.9.14
Доступ на чтение 2.9.15
Доступ при отказе 2.6.16
Доступность 2.2.3
Доступность информационной сферы сети телекоммуникаций 2.14.6
Журнал аудита 2.12.8
Заархивированный файл 2.17.4
Загрязнение 2.6.17
Задание по безопасности 2.3.2
Закладочное устройство 2.6.18
Законодательные средства защиты информации 2.13.3
Замещение 2.8.11
Замкнутая безопасная среда 2.10.2
Запасной пункт обработки данных 2.17.5
Заполнение трафика 2.6.45
Засекречивание сведений и их носителей 2.16.7
Защита данных 2.5.3
Защита информации 2.5.3
Защита информации от несанкционированного доступа . . 2.5.4
Защита от копирования 2.18.5
Защита от несанкционированного доступа 2.10.3
Защита приватности 2.12.9
Защита файла 2.17.6
Защищаемые помещения 2.16.8
Защищенная сеть телекоммуникаций 2.14.7
Защищенное средство вычислительной техники 2.1.4
Защищенное техническое средство информатизации 2.1.5
Защищенность информационной сферы сети телекоммуникаций 2.14.8

Злоумышленник 2.1.6
Зона безопасности 2.10.4
ЗП 2.16.8
Идентификатор 2.9.16
Идентификатор доступа 2.9.17
Идентификатор пользователя 2.9.18
Идентификация 2.9.19
Идентификация риска 2.7.3
Идентификация терминала 2.9.20
Информационная безопасность 2.1.7
Информационная безопасность сети телекоммуникаций . 2.14.9
Информационная инфраструктура сети телекоммуникаций 2.14.10
Информационная сфера сети телекоммуникаций 2.14.11
Информационные ресурсы сети телекоммуникаций 2.14.12
Информация аутентификации 2.9.21
Информация ограниченного доступа 2.5.5
Инцидент 2.1.8
Инцидент информационной безопасности 2.1.9
Искажение информации 2.6.19
Использование ловушек 2.12.10
Категория безопасности 2.5.6
Категория допуска 2.9.22
Категория доступа 2.9.23
Качество обслуживания сети телекоммуникаций в условиях возможных воздействий нарушителя 2.14.13
Качество службы информационной безопасности сети телекоммуникаций 2.14.14
Класс защищенности автоматизированной системы 2.3.3
Класс защищенности средств вычислительной техники . . 2.3.3
Клонирование 2.6.20
Ключ 2.11.3
Код аутентификации сообщений 2.12.11
Код обнаружения манипуляций 2.12.12
Код обнаружения модификаций 2.12.12
Кодирование 2.11.17
Коммерческая тайна 2.16.9
Коммуникационная безопасность 2.1.10
Комплекс средств защиты 2.13.4
Компоновка 2.6.21
Компрометация 2.6.22
Компьютерная безопасность 2.1.11
Компьютерное злоупотребление 2.6.23
Компьютерное мошенничество 2.6.24

Компьютерное преступление 2.6.25
Компьютерный взлом 2.6.26
Контрмера 2.12.13
Контролируемая зона 2.16.10
Контроль нажатия клавиш 2.12.14
Контрольный код 2.18.6
Конфиденциальная информация 2.5.7
Конфиденциальность 2.2.4
Конфиденциальность информационной сферы сети телекоммуникаций 2.14.15
Концепция диспетчера доступа 2.9.24
Косвенная атака 2.8.12
Криптоалгоритм 2.11.7
Криптоанализ 2.11.4
Криптоаналитическая атака 2.8.2
Криптографическая защита информации 2.11.5
Криптографическая система 2.11.6
Криптографический алгоритм 2.11.7
Криптографический метод защиты информации 2.10.5
Криптография 2.11.8
Криптография с открытым ключом 2.11.1
Криптосистема 2.11.6
Критерии риска 2.7.4
Критичная информация 2.5.9
Критичность 2.5.10
КСЗ 2.13.4
Лазейка 2.6.7
Личный ключ 2.11.9
Лобовая атака 2.8.7
Логическая бомба 2.6.27
Логический объект 2.1.12
Логическое управление доступом 2.9.25
Ложная разметка 2.18.7
Ложный сектор 2.18.8
Люк 2.6.28
Мандат 2.9.26
Мандатное управление доступом 2.9.27
Маскарад 2.6.29
Маскировка 2.10.6
Матрица доступа 2.9.28
Международный идентификатор абонента 2.15.1
Межсетевой экран 2.13.5

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, SIFAT VA
NAZORATNI KUCHAYTIRISH
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH DEPARTAMENTI

Меры обеспечения информационной безопасности сети телекоммуникаций 2.14.16
Метка конфиденциальности 2.5.8
Механизм обеспечения информационной безопасности сети телекоммуникаций 2.14.17
Минимум привилегий 2.9.29
Многоуровневая защита 2.10.7
Многоуровневое устройство 2.13.6
Мобильный код сети 2.15.2
Мобильный код страны 2.15.3
Модель защиты 2.3.4
Модель нарушителя правил разграничения доступа 2.9.30
Модель угроз 2.6.30
Модификация информации 2.6.31
Модуль идентификации абонента 2.15.4
Мониторинг системы обеспечения информационной безопасности сети телекоммуникаций 2.14.18
Мониторинг событий информационной безопасности сети телекоммуникаций 2.14.19
Морально-этические средства защиты информации 2.13.7
Мошенничество 2.6.32
Нарушение защиты 2.6.33
Нарушитель 2.1.6
Нарушитель информационной безопасности сети телекоммуникаций 2.14.20
Нарушитель правил разграничения доступа 2.9.31
Неавторизованная попытка доступа к информации 2.8.13
Недекларированные возможности 2.8.14
Незащищенность 2.6.34
Необратимое кодирование 2.11.10
Необратимое шифрование 2.11.10
Неотказуемость 2.2.5
Непосредственная атака 2.8.15
Непризнание участия 2.12.15
Несанкционированное действие 2.6.35
Несанкционированный доступ 2.6.36
Несанкционированный доступ к информации 2.9.32
Несанкционированный доступ к секретной информации . 2.16.11
Несанкционированный доступ к сети телекоммуникаций 2.14.21
Носители сведений, составляющих государственные секреты 2.16.12
Нотаризация 2.12.16
НСД 2.6.36

Обман 2.6.37
Обмен аутентификацией 2.9.33
Обнаружение манипуляций 2.12.17
Обнаружение модификаций 2.12.17
Обобщение 2.6.21
Обработка информации 2.1.13
Обработка рисков 2.7.5
Обратное восстановление 2.17.7
Обратный вызов 2.12.18
Обратный набор 2.12.18
Объект 2.1.14
Объект доступа 2.9.34
Объект информатизации 2.1.15
Объект информационной безопасности сети телекоммуникаций 2.14.22
Одностороннее шифрование 2.11.10
Одноуровневое устройство 2.13.8
Определение рисков 2.7.6
Организационные средства защиты информации 2.13.9
Остаточная информация 2.1.16
Остаточные данные 2.12.19
Остаточный риск 2.7.7
Отказ в обслуживании 2.6.38
Отказоустойчивый 2.12.20
Открытая безопасная среда 2.10.8
Открытый ключ 2.11.11
Открытый текст 2.11.12
Оценка рисков 2.7.8
Очистка 2.12.21
Пароль 2.9.35
Пассивная атака 2.8.16
Пассивная угроза 2.6.39
Пассивный перехват информации 2.6.40
Переполнение 2.6.41
Перестановка 2.11.13
Перехват информации 2.6.42
Перечень сведений, подлежащих засекречиванию в Республике Узбекистан 2.16.13
Период доступа 2.9.36
Персональный идентификационный номер 2.15.5
Персональный ключ разблокировки 2.15.6
ПИН-код 2.15.5
План восстановления 2.17.8
План действий при чрезвычайных ситуациях 2.17.8

O‘zDSt STANDARTLASHTIRISH NAZORATINI ELEKTRON NUSXASI

Побочное излучение 2.6.43
Подделка информации 2.6.44
Подлинность 2.2.1
Подотчетность 2.2.6
Подотчетность информационной сферы сети телекоммуникаций 2.14.23
Подстановка 2.11.14
Подстановка трафика 2.6.45
Подтверждение подлинности личности 2.9.5
Показатели защищенности автоматизированной системы 2.3.5
Показатели защищенности средств вычислительной техники 2.3.5
Политика безопасности 2.3.6
Политика информациионной безопасности сети телекоммуникаций 2.14.24
Политика управления доступом 2.9.37
Полномочие 2.9.38
Полный анализ рисков 2.7.9
Пользователь информации 2.1.17
Понижение категории безопасности 2.12.22
Порядок действий в чрезвычайных ситуациях 2.12.23
Потребитель информации 2.1.17
Почтовый червь 2.6.46
Правила разграничения доступа 2.9.39
Право доступа к записи 2.9.40
Право доступа к чтению 2.9.41
Право на доступ 2.9.42
Преднамеренные угрозы 2.6.47
Препятствие 2.10.9
Прерывание соединения 2.6.48
Приватность 2.1.18
Принуждение 2.10.10
Принцип «положено знать» 2.9.43
Принятие риска 2.7.10
Проверка достоверности данных 2.12.24
Проверочный код 2.18.6
Программная закладка 2.6.49
Программное пиратство 2.6.50
Программное средство защиты информации 2.13.10
Программный вирус 2.6.51
Программный токен 2.9.44
Продажа вызовов 2.6.52
Проникновение 2.6.53

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH DAVLAT
MAZKUR HUJJAT
AKSIGOT TEKSHIRILGAN

Прослушивание 2.6.54
Профиль защиты 2.3.7
Профиль пользователя 2.9.45
Процедура резервирования 2.17.9
Процедурная безопасность 2.1.1
Процедурное мошенничество 2.6.55
Процесс управления риском 2.7.11
Прошивка сети 2.6.56
Прямое восстановление 2.17.10
Разглашение секретных сведений 2.16.14
Разграничение обязанностей 2.12.25
Разделение 2.10.11
Разрешение на доступ 2.9.46
Разрушение секретной информации в средствах вычислительной техники 2.16.15
Раскрытие 2.6.57
Распределенный отказ в обслуживании 2.6.58
Рассекречивание сведений и их носителей 2.16.16
Рассылка спама 2.6.59
Регистрация деятельности 2.9.47
.
Регистрация пользователя 2.9.48
Регламентация 2.10.12
Режим разграничения доступа 2.16.17
Режим секретности 2.16.18
Режимно-секретный орган 2.16.19
Режимные объекты 2.16.20
Резервный пункт обработки данных 2.17.11
Резервный файл 2.17.12
Реконструкция данных 2.17.13
Реставрация данных 2.17.14
Риск 2.7.12
Риск информационной безопасности сети телекоммуникаций 2.14.25
Руководящий орган системы обеспечения информационной безопасности сети телекоммуникаций 2.14.1
Санкционированный доступ к информации 2.9.49
Сбор мусора 2.6.60
Сведения особой важности 2.16.21
СВТ 2.1.21
Секретная работа 2.16.22
Секретные сведения 2.16.23
Секретный ключ 2.11.15
Сертификация 2.4.4

СЗИ НСД 2.4.5
Сигнатура вируса 2.12.26
Симметричная криптография 2.11.16
Система обеспечения информационной безопасности сети телекоммуникаций 2.14.26
Система защиты данных 2.13.11
Система защиты информации 2.13.11
Система защиты информации от несанкционированного доступа 2.4.5
Система обеспечения информационной безопасности . . . 2.4.6
Система разграничения доступа 2.9.50
Система управления доступом 2.9.51
Система управления информационной безопасностью 2.4.7
Система шифрования 2.11.6
Скрытый канал 2.6.61
Слабый бит 2.18.9
Служба информационной безопасности сети телекоммуникаций 2.14.27
Служба обеспечения информационной безопасности 2.4.8
Служебная тайна 2.16.24
Случайные угрозы 2.6.62
Сменный модуль идентификации абонента 2.15.7
Смещенная дорожка 2.18.10
Событие 2.1.19
Событие информационной безопасности 2.1.20
Совершенно секретные сведения 2.16.25
Социальная инженерия 2.6.63
Спиральная дорожка 2.18.11
Список полномочий 2.9.52
Список управления доступом 2.9.53
Способ защиты информации 2.10.13
Спуфинг 2.8.17
СРД 2.9.50
Средства вычислительной техники 2.1.21
Средства защиты информации от несанкционированного доступа 2.13.13
Средства имитозащиты 2.13.14
Средства кодирования 2.13.15
Средства технической защиты информации 2.13.16
Средства шифрования 2.13.17
Средства электронной цифровой подписи 2.13.18
Средство защиты 2.12.27
Средство криптографической защиты информации 2.13.19
Стратегия защиты 2.3.8

Субъект 2.1.22
Субъект доступа 2.9.54
Субъект информационной безопасности сети телекоммуникаций 2.14.28
СУД 2.9.51
СУИБ 2.4.7
Суперсектор 2.18.12
Телефонный пират. 2.14.29
Тестирование на проникновение 2.12.28
Техническая защита информации 2.10.14
Технические средства защиты информации 2.13.20
Технические средства информатизации 2.1.23
Технологическая безопасность сети телекоммуникаций . 2.14.30
Точка доступа к сети 2.9.55
Троянская программа 2.6.64
ТСИ 2.1.23
Угроза 2.6.65
Угроза информационной безопасности сети телекоммуникаций 2.14.31
Универсальный модуль идентификации абонента 2.15.6
Уничтожение информации 2.6.66
Управление доступом 2.9.56
Управление рисками 2.7.13
Уровень безопасности 2.3.9
Уровень доступа 2.9.57
Уровень информационной безопасности сети телекоммуникаций 2.14.32
Уровень полномочий субъекта доступа 2.9.58
Уровень риска 2.7.14
Услуга управления доступом 2.9.59
Устойчивость функционирования сети телекоммуникаций 2.14.33
Утечка секретной информации 2.16.26
Утрата документов или изделий, содержащих секретные сведения 2.16.27
Утрата предметов, содержащих секретные сведения 2.16.27
Ущерб 2.6.67
Уязвимость 2.6.68
Уязвимость информации 2.6.69
Уязвимость сети телекоммуникаций 2.14.34
Фактор, воздействующий на защищаемую информацию . 2.6.70
Физическая защита 2.13.21
Физическая угроза 2.6.71
Физические средства защиты 2.13.22

O‘ZSTANDART
STANDARTLASHTIRISH
MAZORATINI
AXBOROT

Физический пиггибекинг 2.6.72
Физическое управление доступом 2.9.60
Фильтр безопасности 2.12.29
Фрикер 2.14.29
Холодный резерв 2.17.5
Целостность 2.2.7
Целостность информационной сферы сети телекоммуникаций 2.14.35
Целостность системы 2.2.8
Цель обеспечения информационной безопасности сети телекоммуникаций 2.14.36
Цифровая подпись 2.12.30
Цифровой конверт 2.12.31
Червь 2.6.73
Чувствительная информация 2.5.9
Чувствительность 2.5.10
Широкая дорожка 2.18.13
Шифрование 2.11.17
Шифротекст 2.11.18
Экранирование 2.10.15
Эксплуатационная безопасность сети телекоммуникаций 2.14.37
Эксплуатационный люк 2.6.74
Электронный пиггибекинг 2.6.75
Эшелонированная защита 2.3.10
Ядро защиты 2.9.10
SIM-карта 2.15.4

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH ... INSTITUTI
NAZORAT ... BO‘LIMI
AXBOROT ... BO‘LIMI
JORIY ETISH ...

4 Алфавитный указатель терминов на узбекском языке

Абонентни идентификация қилиш модули 2.15.4
Абонентни идентификация қилишнинг алмаштириладиган модули 2.15.7
Абонентни идентификация қилишнинг универсал модули 2.15.8
Абонентнинг халқаро идентификатори 2.15.1
Автоматлаштирилган тизимнинг муҳофаза қилинганлик класси 2.3.3
Автоматлаштирилган тизимнинг муҳофаза қилинганлик кўрсаткичи 2.3.5
Агрегирлаш 2.6.1
Ажратиш 2.10.11
Актив таҳдид 2.6.2
Алдов 2.6.37
Алоқа хавфсизлиги 2.1.10
Алоҳида аҳамиятга молик маълумотлар 2.16.21
АМҚВ 2.13.12
Аналитик ҳужум 2.8.2
Антивирусли дастурий таъминот 2.13.1
Аппаратли токен 2.9.3
АРФМТ 2.4.5
Архивга оид файл 2.17.2
Архивлаш 2.17.1
Архивлаштирилган файл 2.17.4
Асимметрик криптография 2.11.1
Аслига тўғрилик 2.2.1
Аудит дафтари 2.12.8
Аутентификация билан алмашиш 2.9.33
Аутентификация қилиш 2.9.4
Аутентификация қилиш ахбороти 2.9.21
Ахборот истеъмолчиси 2.1.17
Ахборот ресурсидан фойдалана олиш 2.9.13
Ахборот (маълумотлар)ни муҳофаза қилиш тизими 2.13.11
Ахборот (маълумотлар) хавфсизлиги 2.5.1
Ахборот модификацияси 2.6.31
Ахборот узатилишини блокировкалаш 2.6.6
Ахборот хавфсизлиги 2.1.7
Ахборот хавфсизлиги инциденти 2.1.9
Ахборот хавфсизлиги ҳодисаси 2.1.20
Ахборот хавфсизлигини бошқариш тизими 2.4.7
Ахборот хавфсизлигини таъминлаш тизими 2.4.6
Ахборот хавфсизлигини таъминлаш хизмати 2.4.8

Ахборотдан муаллифлаштирилмаган тарзда фойдаланишга уриниш 2.8.13
Ахборотдан рухсатсиз фойдалана олиш 2.9.32
Ахборотдан рухсат этилган тарзда фойдалана олиш 2.9.49
Ахборотдан фойдалана олиш 2.9.12
Ахборотдан фойдаланувчи 2.1.17
Ахборотлаштириш объекти 2.1.15
Ахборотлаштириш объектларини аттестатлаш 2.3.1
Ахборотлаштиришни муҳофаза қилинган техник воситаси 2.1.5
Ахборотлаштириш техник воситалари 2.1.23
АТВ 2.1.23
Ахборотни криптографик муҳофаза қилиш 2.11.5
Ахборотни криптографик муҳофаза қилиш воситаси 2.13.19
Ахборотни муҳофаза қилишнинг техник воситалари . . . 2.13.20
Ахборотни сохталаштириш 2.6.44
Ахборотни актив тарзда тутиб олиш 2.6.3
Ахборотни йўқ қилиш 2.6.66
Ахборотни муҳофаза қилиш 2.5.3
Ахборотни муҳофаза қилиш воситалари 2.13.12
АМВ 2.13.12
Ахборотни муҳофаза қилиш усули 2.10.13
Ахборотни муҳофаза қилишнинг қонунлаштирилган воситалари 2.13.3
Ахборотни муҳофаза қилишнинг ташкилий воситалари . 2.13.9
Ахборотни муҳофаза қилишнинг аппарат-дастурий воситалари 2.13.20
Ахборотни муҳофаза қилишнинг аппарат воситаси 2.13.2
Ахборотни муҳофаза қилишнинг дастурий воситаси 2.13.10
Ахборотни муҳофаза қилишнинг криптографик усули . . . 2.10.5
Ахборотни муҳофаза қилишнинг маънавий-аҳлоқий воситалари 2.13.7
Ахборотни пассив тарзда тутиб олиш 2.6.40
Ахборотни техник мухофаза қилиш 2.10.14
Ахборотни техник мухофаза қилиш воситалари 2.13.16
Ахборотни рухсат этилмаган фойдалана олишдан муҳофаза қилиш воситалари 2.13.13
Ахборотни рухсат этилмаган тарзда фойдалана олишдан муҳофаза қилиш 2.5.4
Ахборотни рухсатсиз фойдалана олишдан муҳофаза қилиш тизими 2.4.5
Ахборотни тутиб олиш 2.6.42
Ахборотни қайта ишлаш 2.1.13
Ахборотнинг заифлиги 2.6.69
Ахлат йиғиш 2.6.60

АХТБ 2.4.7
Бевосита тиклаш 2.17.10
Бевосита ҳужум 2.8.15
Билвосита ҳужум 2.8.12
«Билиш зарур» принципи 2.9.43
Биометрик 2.12.4
Бир даражали қурилма 2.13.8
Бир томонлама шифрлаш 2.11.10
Бирин-кетин жойлаштириб муҳофаза килиш 2.3.10
Блокировка қилиш 2.18.1
Блокировкадан чиқаришнинг шахсий калити 2.15.6
Боғланишни узиш 2.6.48
Бузилишларга барқарор 2.12.20
Бузғунчи 2.1.6
Бузғунчининг телекоммуникациялар тармоғига таъсири . 2.14.5
Бузғунчининг телекоммуникациялар тармоғига ҳужуми . 2.14.5
Бузғунчининг эҳтимолий таъсирлари шароитларида телекоммуникациялар тармоғига хизмат кўрсатиш сифати . . 2.14.13
Ваколат 2.9.38
Ваколатлар рўйхати 2.9.52
Валидация 2.12.5
Вақт бомбаси 2.6.12
Верификация 2.12.6
Вирус 2.6.51
Вирус сигнатураси 2.12.26
Вирусга қарши дастур 2.12.1
Давлат сири 2.16.2
Давлат сирлари 2.16.3
Давлат сирларидан фойдаланиш ҳуқуқи 2.16.5
Давлат сирларини ташкил этувчи маълумотлардан фойдалана олиш 2.16.6
Давлат сирларини ташкил этувчи маълумотларни ташувчилар 2.16.12
Дастурий вирус 2.6.51
Дастурий қароқчилик 2.6.50
Дастурий токен 2.9.44
Дастурий ўрнатма 2.6.49
Декодлаш 2.11.2
Декларация қилинмаган имкониятлар 2.8.14
Дестабиллаштирувчи ички омил 2.6.10
Дестабиллаштирувчи омил 2.6.15

O‘ZBEKISTON STANDARTLASHTIRISH NAZORATINI AXBOROT TEXNOLOGIYALARI JORIY ETISH MARKAZI

Дестабиллаштирувчи ташқи омил 2.6.8
Дестабиллаштирувчи таъсир 2.6.14
Дешифрлаш 2.11.2
Ёзиб олишга рухсат 2.9.14
Ёзувдан фойдалана олиш ҳуқуқи 2.9.40
Ёпиқ хавфсиз муҳит 2.10.2
Жиноятқор 2.1.6
Жисмоний муҳофаза қилиш 2.13.21
Жисмоний муҳофаза қилиш воситалари. 2.13.22
Жисмоний пиггибекинг 2.6.72
Жисмоний таҳдид 2.6.71
Заифлик 2.6.68
Зарар 2.6.67
Зарарловчи дастур 2.6.11
Идентификатор 2.9.16
Идентификацион шахсий рақам 2.15.5
Идентификация қилиш 2.9.19
Ижтимоий инженерия 2.6.63
Имитомуҳофаза воситалари 2.13.14
Имтиёзлар минимуми 2.9.29
Инцидент 2.1.8
Иссиқ резерв 2.17.11
Ифлосланиш 2.6.17
Ичига кириб олиш 2.6.53
Ички фирибгарлик 2.6.9
Ички ҳужум 2.8.10
Ишончли компьютер тизими 2.1.3
Ишончли маълумотлар 2.9.7
Ишончлилик 2.2.2
ИШР-код 2.15.5
Иштирокни тан олмаслик 2.12.15
Калит 2.11.3
Кенг йўлка 2.18.13
Клавишлар босилишини назорат қилиш 2.12.14
Клонлаш 2.6.20
Кодлаш 2.11.17
Кодлаш воситалари 2.13.15
Коммуникацион хавфсизлик 2.1.10
Компоновка қилиш 2.6.21
Компрометация (обрўсизлантириш) 2.6.22
Компьютер хавфсизлиги 2.1.11
Компьютер воситасида бузиш (кириш) 2.6.26
Компьютер жинояти 2.6.25
Компьютер суиистеъмоллиги 2.6.23

Компьютер тизимининг аудити 2.12.2
Компьютер фирибгарлиги 2.6.24
Конфиденциал ахборот 2.5.7
Конфиденциаллик 2.2.4
Конфиденциаллик белгиси 2.5.8
Криптоаналитик ҳужум 2.8.2
Криптографик алгоритм 2.11.7
Криптографик алмаштириш алгоритми 2.11.7
Криптографик тизим 2.11.6
Криптография 2.11.8
Криптотаҳлил 2.11.4
Криптотизим 2.11.6
Критик ахборот 2.5.9
Критиклик 2.5.10
Кўп даражали қурилма 2.13.6
Кўп поғонали муҳофаза қилиш 2.10.7
Люк 2.6.28
Мажбуриятларни белгилаш 2.12.25
Мажбурлаш 2.10.10
Мамлакатнинг мобил коди 2.15.3
Мандат 2.9.26
Манипуляцияларни аниқлаш 2.12.17
Манипуляцияларни аниқлаш коди 2.12.12
Мантиқий бомба 2.6.27
Мантиқий объект 2.1.12
Маскарад 2.6.29
Махфий ахборотдан рухсат этилмаган тарзда фойдалана олиш 2.16.11
Махфий ахборотнингчиқиб кетиши. 2.16.26
Махфий иш 2.16.22
Махфий калит 2.11.15
Махфий маълумотлар 2.16.23
Махфий маълумотлар бўлган ҳужжатлар ёки буюмларнинг йўқолиши 2.16.27
Махфий маълумотлар бўлган ҳужжатлар ёки нарсаларнинг йўқолиши 2.16.27
Махфий маълумотларнинг ошкор этилиши. 2.16.14
Махфийлик грифи 2.16.4
Махфий маълумотлар бўлган ҳужжатлар ёки буюмларнинг йўқолиши 2.16.27
Махфий нарсаларнинг йўқолиши 2.16.27
Махфийлик режими 2.16.18
Махфий-режимли орган. 2.16.19
Маълум очиқ матн бўйича ҳужум 2.8.6

Маълумотлар ва уларни ташувчиларини махфийлаштириш 2.16.7
Маълумотлар ва уларнинг ташувчиларини ошкор қилиш 2.16.16
Маълумотлар узатилишини блокировкалаш 2.6.6
Маълумотлар хавфсизлиги 2.5.1
Маълумотларни аутентификация қилиш 2.12.3
Маълумотларни қайта ишлашнинг захира пункти 2.17.5
Маълумотларни қайта ишлашнинг резерв пункти 2.17.11
Маълумотларни муҳофаза қилиш 2.5.3
Маълумотларни реконструкция қилиш 2.17.13
Маълумотларни реставрация қилиш 2.17.14
Маълумотларни янгитдан яратиш 2.17.3
Маълумотларнинг ишончлилигини текшириш 2.12.24
Маъмурий хавфсизлик 2.1.1
МХ 2.16.8
МВК 2.13.4
Модификацияларни аниқлаш 2.12.17
Модификацияларни аниқлаш коди 2.12.12
Муаллифлаштирилган эркин фойдаланиш субъекти 2.9.2
Муаллифлаштириш 2.9.1
Мутлақо махфий маълумотлар 2.16.25
Муҳофаза қилинган автоматлаштирилган тизим 2.1.4
Муҳофаза қилишнинг бузилиши 2.6.33
Муҳофаза қилинадиган ахборотга таъсир кўрсатувчи омил 2.6.70
Муҳофаза қилинадиган хоналар 2.16.8
Муҳофаза қилинган телекоммуникациялар тармоғи 2.14.7
Муҳофаза қилинмаганлик 2.6.34
Муҳофаза қилиш воситалари комплекси. 2.13.4
Муҳофаза қилиш воситаси 2.12.27
Муҳофаза қилиш маъмури 2.4.1
Муҳофаза қилиш модели 2.3.4
Муҳофаза қилиш профили 2.3.7
Муҳофаза қилиш стратегияси 2.3.8
Муҳофаза қилиш тизимининг маъмурий бошқаруви 2.4.2
Муҳофаза қилиш ядроси 2.9.10
Назорат коди 2.18.6
Назорат килинадиган зона 2.16.10
Ниқоблаш 2.10.6
Номақбул нурланиш 2.6.43
Норасмийлик 2.1.18
Норасмийликни муҳофаза қилиш 2.12.9
Нотариаллаштириш 2.12.16
Нусха кўчиришдан муҳофаза қилиш 2.18.5

AXBOROT
JORIY ETISH

Объект 2.1.14
Очиқ калит 2.11.11
Очиқ калитли криптография 2.11.1
Очиқ матн 2.11.12
Очиқ матнни ажратиб бажариладиган ҳужум 2.8.4
Очиқ хавфсиз муҳит 2.10.8
Пароль 2.9.35
Пассив таҳдид 2.6.39
Пассив ҳужум 2.8.16
Почта қурти 2.6.46
Процедура фирибгарлиги 2.6.55
Процедура хавфсизлиги 2.1.1
Рад этиш вақтидаги фойдаланиш 2.6.16
Рад этолмаслик 2.2.5
Рақамли имзо 2.12.30
Рақамли конверт 2.12.31
Режимли объектлар 2.16.20
Резерв файл 2.17.12
Резервлаш процедураси 2.17.9
Риск 2.7.12
Риск даражаси 2.7.14
Риск мезонлари 2.7.4
Риск таҳлили 2.7.1
Рискларни аниқлаш 2.7.6
Рискларни баҳолаш 2.7.8
Рискларни бошқариш 2.7.13
Рискни бошқариш жараёни 2.7.11
Рискларнинг асосий таҳлили 2.7.2
Рискларни тўлик таҳлил қилиш 2.7.9
Рискни қабул қилиш 2.7.10
Рискни қайта ишлаш 2.7.5
Рискни идентификация қилиш 2.7.3
Рухсатсиз фойдалана олишдан муҳофаза қилиш 2.10.3
Рухсат бериш 2.9.22
Рухсат бериш категорияси 2.9.22
Рухсатсиз фойдалана олиш 2.6.36
Рухсатсиз фаолият 2.6.35
РФО 2.6.36
Рўпарадан қилинган ҳужум 2.8.7
Сатрлар орасига кириш 2.6.13
Секторни тўғрилаш 2.18.2
Сертификатлаш 2.4.4
Силжиган йўлка 2.18.10
Симметрик криптография 2.11.16

O'ZSTANDART
STANDARTLASHTIRISH
MUVOFIQLIKNI
AXBOROT TEXNO
JORIY

Совуқ резерв 2.17.5
Спамни жўнатиш 2.6.59
Спираль йўлка 2.18.11
Спуфинг 2.8.17
Субъект 2.1.22
Суперсектор 2.18.12
Суст бит 2.18.9
Суқулиб кириш имкониятини тестлаш 2.12.28
Тармоқдан фойдалана олиш нуқтаси 2.9.55
Тармоқлараро экран 2.13.5
Тармоқни тешиб ўтиш 2.6.56
Тармоқнинг мобил коди 2.15.2
Тартибга солиш 2.10.12
Тасодифий таҳдидлар 2.6.62
Таҳдид 2.6.65
Таҳдидлар модели 2.6.30
Таҳдидларни таҳлил қилиш 2.6.5
Таъсирчан ахборот 2.5.9
Таъсирчанлик. 2.5.10
Текшириш коди 2.18.6
Телекоммуникациялар тармоғи ахборот соҳасининг конфиденциаллиги 2.14.15
Телекоммуникациялар тармоғи ахборот хавфсизлиги хизматининг сифати 2.14.14
Телекоммуникациялар тармоғи ахборот хавфсизлигини таъминлаш тизимининг мониторинги 2.14.18
Телекоммуникациялар тармоғининг ахборот хавфсизлигини таъминлаш тизимининг раҳбарий органи 2.14.1
Телекоммуникациялар тармоғининг ахборот хавфсизлиги риски 2.14.25
Телекоммуникациялар тармоғининг ахборот хавфсизлигини таъминлаш тизими 2.14.26
Телекоммуникациялар тармоғининг заифлиги 2.14.34
Телекоммуникациялар тармоғининг ахборот хавфсизлиги хизмати 2.14.27
Телекоммуникациялар тармоғи ахборот соҳасидан фойдалана олишлик 2.14.6
Телекоммуникациялар тармоғи ахборот соҳасидан тайёрлиги 2.14.6
Телекоммуникациялар тармоғи ахборот соҳасининг муҳофаза қилинганлиги 2.14.8
Телекоммуникациялар тармоғи ахборот соҳасининг яхлитлиги 2.14.35

O'ZBEKISTON STANDARTLARI AXBOROT FONDI
RASMIY ETUSH UCHUN

Телекоммуникациялар тармоғи ахборот соҳасининг ҳисоб беришлиги 2.14.23
Телекоммуникациялар тармоғи ахборот хавфсизлигининг бузғунчиси 2.14.20
Телекоммуникациялар тармоғи ахборот хавфсизлигининг таянч даражаси 2.14.3
Телекоммуникациялар тармоғи ахборот хавфсизлигини таъминлаш тизимининг архитектураси 2.14.2
Телекоммуникациялар тармоғи ахборот хавфсизлигини таъминлаш тизимининг маъмури 2.14.1
Телекоммуникациялар тармоғи ахборот хавфсизли-ги ҳодисаларининг мониторинги 2.14.19
Телекоммуникациялар тармоғи ишлашининг барқарорлиги 2.14.33
Телекоммуникациялар тармоғидан рухсатсиз фойдалана олиш 2.14.21
Телекоммуникациялар тармоғидан фойдаланиш хавфсизлиги 2.14.37
Телекоммуникациялар тармоғининг хавфсизлиги 2.14.4
Телекоммуникациялар тармоғининг ахборот инфраструктураси 2.14.10
Телекоммуникациялар тармоғининг ахборот ресурслари 2.14.12
Телекоммуникациялар тармоғининг ахборот соҳаси 2.14.11
Телекоммуникациялар тармоғининг ахборот хавфсизлиги 2.14.9
Телекоммуникациялар тармоғининг ахборот хавфсизлиги объекти 2.14.22
Телекоммуникациялар тармоғининг ахборот хавфсизлиги даражаси 2.14.32
Телекоммуникациялар тармоғининг ахборот хавфсизлиг сиёсати 2.14.24
Телекоммуникациялар тармоғининг ахборот хавфсизлиги субъекти 2.14.28
Телекоммуникациялар тармоғининг ахборот хавфсизлигига таҳдид 2.14.31
Телекоммуникациялар тармоғининг ахборот хавфсизлигини таъминлаш чоралари 2.14.16
Телекоммуникациялар тармоғининг ахборот хавфсизлигини таъминлаш механизми 2.14.17
Телекоммуникациялар тармоғининг ахборот хавфсизлигини таъминлаш мақсади 2.14.36
Телекоммуникациялар тармоғининг технологик хавфсизлиги 2.14.30
Телефон қароқчиси 2.14.29

Терминални идентификация қилиш 2.9.20
Тешик 2.6.7
Тижорат сири 2.16.9
Тизимнинг яхлитлиги 2.2.8
Тиклаш режаси 2.17.8
Тозалаш 2.12.21
Трафикни таҳлил қилиш. 2.6.4
Трафикни тўлдириш 2.6.45
Трафикни ўрнига қўйиш 2.6.45
Троян дастури 2.6.64
Туйнук 2.6.7
Тўлдириб юбориш ҳужуми 2.8.5
Тўлдириш 2.6.41
Тўлиқ ажратиб бажариладиган ҳужум 2.8.7
Тўсқинлик 2.10.9
Умумлаштириш 2.6.21
Фавқулодда вазиятларда ҳаракат қилиш режаси 2.17.8
Фавқулодда вазиятларда ҳаракат қилиш тартиби 2.12.23
Файлни муҳофаза қилиш 2.17.6
Фаол ҳужум 2.8.1
Фаолиятни қайд қилиш 2.9.47
Фақат шифрланган матн бўйича ҳужум 2.8.9
ФБТ 2.9.51
Фирибгарлик 2.6.32
Фойдалана олиш 2.9.11
Фойдалана олиш идентификатори 2.9.17
Фойдалана олиш матрицаси 2.9.28
Фойдалана олиш объекти 2.9.34
Фойдалана олиниши чекланган ахборот 2.5.5
Фойдалана олишлик 2.2.3
Фойдалана олишни бошқариш 2.9.56
Фойдалана олишни бошқариш рўйхати 2.9.53
Фойдалана олишни бошқариш сиёсати 2.9.37
Фойдалана олишни бошқариш хизмати 2.9.59
Фойдалана олишни дискрецион бошқариш 2.9.9
Фойдалана олишни мандатли бошқариш 2.9.27
Фойдалана олиш диспетчери 2.9.10
Фойдалана олиш диспетчери концепцияси 2.9.24
Фойдалана олиш субъектлари ваколатлари даражаси 2.9.58
Фойдалана олишни чегаралаш тизими 2.9.50
Фойдалана олишни чеклаш қоидалари 2.9.39
Фойдалана олишни чегаралаш қоидаларини бузувчи . . . 2.9.31
Фойдалана олишни чегаралаш қоидаларини бузувчининг модели 2.9.30

Фойдалана олишни чеклаш режими. 2.16.17
Фойдалана олиш субъекти 2.9.54
Фойдалана олиш категорияси 2.9.23
Фойдалана олиш даври 2.9.36
Фойдалана олиш даражаси 2.9.57
Фойдаланиш тури 2.9.8
Фойдалана олиш ҳуқуқи 2.9.42
Фойдаланишга рухсат 2.9.46
Фойдалана олишни бошқариш тизими 2.9.51
Фойдалана олишни жисмонан бошқариш 2.9.60
Фойдаланишни мантиқий бошқариш 2.9.25
Фойдаланувчини рўйхатга олиш 2.9.48
Фойдаланувчининг идентификатори 2.9.18
Фойдаланувчининг профили 2.9.45
Фош этиш 2.6.57
Фрикер 2.14.29
ФЧТ 2.9.50
Хабарларни аутентификация қилиш коди 2.12.11
Хабарни аутентификация қилиш 2.9.6
Хавфсизлик 2.1.2
Хавфсизлик аудити 2.4.3
Хавфсизлик бўйича топшириқ 2.3.2
Хавфсизлик даражаси 2.3.9
Хавфсизлик домени 2.10.1
Хавфсизлик зонаси 2.10.4
Хавфсизлик категорияси 2.5.6
Хавфсизлик категориясини пасайтириш 2.12.22
Хавфсизлик маъмури 2.4.1
Хавфсизлик сиёсати 2.3.6
Хавфсизлик фильтри 2.12.29
Хизмат кўрсатишни рад этиш 2.6.38
«Хизмат кўрсатишни рад этиш» туридаги ҳужум 2.8.8
Хизмат кўрсатишни тақсимланган рад этиш 2.6.58
Хизматга доир сир 2.16.24
Чақирувларни сотиш 2.6.52
Чалғитувчи белги 2.18.7
Чалғитувчи сектор 2.18.8
Шахсий калит 2.11.9
Шахсни аутентификация қилиш 2.9.5
Шахснинг ҳақиқийлигини тасдиқлаш 2.9.5
Шифрланган матн 2.11.18
Шифрлаш 2.11.17
Шифрлаш воситалари 2.13.17
Шифрлаш тизими 2.11.6

O‘ZSTANDART
STANDARTLASHTIRISH
MAZORATINI
AXBOROT
JORIY ETISH

Экранлаштириш 2.10.15
Эксплуатация қилиш люки 2.6.74
Электрон пиггибекинг 2.6.75
Электрон рақамли имзо воситалари 2.13.18
Эшитиш 2.6.54
Яхлитлик. 2.2.7
Яширин канал 2.6.61
Ўзаро ишончсизлик 2.12.17
Ўзбекистон Республикасида махфийлаштирилиши лозим бўлган маълумотлар рўйхати 2.16.13
Ўқиш имкониятини олиш ҳуқуқи 2.9.41
Ўқиш учун рухсат 2.9.15
Ўрнатилган қурилма 2.6.18
Ўрнига қўйиш 2.11.14
Ўрнини алмаштириш 2.11.13
Ўрнини босиш 2.8.11
Қайта рақам териш 2.12.18
Қайта чақириш 2.12.18
Қайтарилмайдиган кодлаш 2.11.10
Қайтарилмайдиган шифрлаш 2.11.10
Қайта тиклаш 2.17.7
Қарши чора 2.12.13
Қасддан қилинадиган таҳдидлар 2.6.47
Қолдиқ маълумотлар 2.12.19
Қолдиқ ахборот 2.1.16
Қолдиқ риск 2.7.7
Қопқонлардан фойдаланиш 2.12.10
Курт 2.6.73
Қўшимча йўлка 2.18.3
Қўшимча сектор 2.18.4
Ҳақиқийлик 2.2.1
Ҳарбий сир 2.16.1
Ҳисоб беришлик 2.2.6
Ҳисоблаш техникаси воситалари 2.1.21
ҲТВ 2.1.21
Ҳисоблаш техникаси воситаларида махфий ахборотнинг бузилиши 2.16.15
Ҳисоблаш техникаси воситаларининг муҳофаза қилинганлик класси 2.3.3
Ҳисоблаш техникаси воситаларининг муҳофаза қилинганлик кўрсаткичи 2.3.5
Ҳисоблаш техникасининг муҳофаза қилинган воситаси . . 2.1.4
Ҳодиса 2.1.19
Ҳужжат 2.5.2

Ҳужжатлаштирилган ахборот 2.5.2
Ҳужум 2.8.3
SIM-карта 2.15.4

O‘ZSTANDART AXBOROT
STANDARTLASHTIRISH
MILLIY
MAZMUNAN
AXBOROT TEXNOLOGIYALARI

5 Алфавитный указатель терминов на английском языке

Aborted connection 2.6.48
Access 2.9.11
Access category 2.9.23
Access control 2.9.56
Access control list 2.9.53
Access control policy 2.9.37
Access control service 2.9.59
Access demarcation mode 2.16.17
Access identifier 2.9.17
Access level 2.9.57
Access matrix 2.9.28
Access object 2.9.34
Access period 2.9.36
Access permission 2.9.46
Access right 2.9.42
Access subject 2.9.54
Access to information 2.9.12
Access to information resource 2.9.13
Access to state secret 2.16.5
Access to state secret information 2.16.6
Access type 2.9.8
Accidental threats 2.6.62
Accountability 2.2.6
Accountability of information sphere of telecommunication network 2.14.23
Action of intruder on telecommunication network 2.14.5
Active attack 2.8.1
Active threat 2.6.2
Active wiretapping 2.6.3
Activity registration 2.9.47
Administrative security 2.1.1
Administrator of system of information security of telecommunication network 2.14.1
Aggregation 2.6.1
Analytical attack 2.8.2
Antivirus program 2.12.1
Antivirus software 2.13.1
Architecture of system of information security of telecommunication network 2.14.2
Archive file 2.17.2
Archived file 2.17.4

Archiving 2.17.1
Asymmetric cryptography 2.11.1
Attack 2.8.3
Attack of intruder on telecommunication network 2.14.5
Attempt of unauthorised access to information 2.8.13
Audit trail 2.12.8
Authentication 2.9.4
Authentication exchange 2.9.33
Authentication information 2.9.21
Authenticity 2.2.1
Authorization 2.9.1
Authorized access subject 2.9.2
Authorized access to information 2.9.49
Availability 2.2.3
Availability of information sphere of telecommunication network 2.14.6
Backup file 2.17.12
Backup procedure 2.17.9
Backward recovery 2.17.7
Bad sectoring 2.18.7
Base level of information security of telecommunication network 2.14.3
Baseline risk analysis 2.7.2
Bearers of state secrets 2.16.12
Between-the-lines entry 2.6.13
Biometric 2.12.4
Breach 2.6.33
Brute-force attack 2.8.7
Bug device 2.6.18
Call selling 2.6.52
Call-back 2.12.18
Capability 2.9.38
Capability list 2.9.52
CAS 2.9.51
Certification 2.4.4
Checking code 2.18.6
Chosen-plaintext attack 2.8.4
Ciphersystem 2.11.6
Ciphertext 2.11.18
Ciphertext-only attack 2.8.9
Classification of information and its bearers as secret 2.16.7
Clearance 2.9.22
Clearing 2.12.21

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH ... DAVLAT
NAZORATINI ... XIZMATI
ANDOZOT ... TEXNIK ...
JORIY ETILGAN ...

Cleartext 2.11.12
Cloning 2.6.20
Closed-security environment 2.10.2
Coding tools 2.13.15
Cold site 2.17.5
Communications security 2.1.10
Compartmentalization 2.10.11
Compromise 2.6.22
Compromising emanation 2.6.43
Computer abuse 2.6.23
Computer crime 2.6.25
Computer fraud 2.6.24
Computer security 2.1.11
Computer-system audit 2.12.2
Confidential information 2.5.7
Confidentiality 2.2.4
Confidentiality mark 2.5.8
Confidentiality of information sphere of telecommunication network 2.14.15
Contamination 2.6.17
Contingency plan disaster 2.17.8
Contingency procedure 2.12.23
Controlled access system 2.9.51
Controlled zone 2.16.10
Copy protection 2.18.5
Countermeasure 2.12.13
Covert channel 2.6.61
Cracking 2.6.26
Credentials 2.9.7
Cryptanalysis 2.11.4
Cryptanalytical attack 2.8.2
Cryptographic algorithm 2.11.7
Cryptographic information protection facility 2.13.19
Cryptographic method of information protection 2.10.5
Cryptographic protection to information 2.11.5
Cryptographic system 2.11.6
Cryptography 2.11.8
Cryptosystem 2.11.6
Data authentication 2.12.3
Data destruction 2.6.66
Data falsification 2.6.44
Data protection system 2.13.11
Data reconstitution 2.17.3
Data reconstruction 2.17.13

Data restoration 2.17.14
Data transmission blocking 2.6.6
Data validation 2.12.24
Decipherment 2.11.2
Declassification of information and its bearers as secret 2.16.16
Decryption 2.11.2
Defence-in-depth 2.3.10
Degree of classification 2.16.4
Denial of Service 2.6.38
Denial of service attack 2.8.8
Destabilizing impact 2.6.14
Destabilizing factor 2.6.15
Destruction of secret information in facility of computing machinery 2.16.15
Dial-back 2.12.18
Digital envelope 2.12.31
Digital signature 2.12.30
Direct attack 2.8.15
Disclosure 2.6.57
Disclosure of secret information 2.16.14
Discretionary access control 2.9.9
Distributed Denial of Service 2.6.58
Document 2.5.2
Documented information 2.5.2
Eavesdropping 2.6.54
Email-worm 2.6.46
Encipherment 2.11.17
Encryption 2.11.17
Enforcement 2.10.10
Entity 2.1.12
Entrapment 2.12.10
Event 2.1.19
Event of information security 2.1.20
Exhaustive attack 2.8.7
Exposure 2.6.34
External destabilizing factor 2.6.8
Extra sector 2.18.4
Extra track 2.18.3
Facilities of computing machinery 2.1.21
Facilities of electronic digital signature 2.13.18
Facilities of technical protection of information 2.13.16
Facilities of cryptooperation 2.13.17
Factor, acting upon protectable information 2.6.70

O'ZBEKISTON STANDARTLASHTIRISH, METROLOGIYA VA SERTIFIKATLASHTIRISH AGENTLIGI

Failsafe 2.12.20
Failure access 2.6.16
Fake sector 2.18.8
File protection 2.17.6
Firewall 2.13.5
Flaw 2.6.7
Flooding 2.6.41
Flooding attack 2.8.5
Forward recovery 2.17.10
Fraud 2.6.32
Full risk analysis 2.7.9
Fusion 2.6.21
Garbage collection 2.6.60
Governing body of system of information security of telecommunication network 2.14.1
Guard 2.12.27
Hacker 2.1.6
Hacking 2.8.13
Hard token 2.9.3
Hardware and software protection means 2.13.20
Highly important information 2.16.21
Hot site 2.17.11
Hot standby 2.17.11
Identification 2.9.19
Identifier 2.9.16
Identity authentication 2.9.5
Identity validation 2.9.5
Imitoprotection means 2.13.14
Incident 2.1.8
Incident of information security 2.1.9
Indirect attack 2.8.12
Information distortion 2.6.19
Information infrastructure of telecommunication network . . 2.14.10
Information modification 2.6.31
Information processing 2.1.13
Information protection system 2.13.11
Information resources of telecommunication network 2.14.12
Information security 2.1.7
Information security hardware 2.13.2
Information security management system 2.4.7
Information security of telecommunication network 2.14.9
Information security software 2.13.10
Information security system 2.4.6
Information sphere of telecommunication network 2.14.11

Information transmission blocking 2.6.6
Information user 2.1.17
Integrity 2.2.7
Integrity of information sphere of telecommunication network 2.14.35
Intentional threats 2.6.47
Internal destabilizing factor 2.6.10
Internal fraud 2.6.9
International Mobile Subscriber Identity 2.15.1
Intruder 2.1.6
Intruder of information security of telecommunication network 2.14.20
Irreversible encipherment 2.11.10
Irreversible encryption 2.11.10
ISMS 2.4.7
Key 2.11.3
Keystroke verification 2.12.14
Known-plaintext attack 2.8.6
Legal protection means 2.13.3
Level of information security of telecommunications network 2.14.32
Level of risk 2.7.14
Limited access information 2.5.5
Linkage 2.6.21
List of information to be classified as secret in Republic of Uzbekistan 2.16.13
Logic bomb 2.6.27
Logical access control 2.9.25
Loophole 2.6.7
Loss 2.6.67
Loss of documents or products, containing secret information 2.16.27
Loss of units, containing secret information 2.16.27
Maintenance hook 2.6.74
Maintenance security of telecommunication network 2.14.37
Malicious logic 2.6.11
Mandatory access control 2.9.27
Manipulation detection 2.12.17
Manipulation detection code 2.12.12
Masking 2.10.6
Masquerade 2.6.29
Measures of information security of telecommunication network 2.14.16

O'ZSTANDART AJ ...
STANDARTLASHTIRISH ...
NAZORATINI ...
AXBOROT ...
JORIY ...

Mechanism of information security of telecommunication network 2.14.17
Message authentication 2.9.6
Message authentication code 2.12.11
Method of protection of information 2.10.13
Military secret 2.16.1
Minimum privilege 2.9.29
Mobile Network Code 2.15.2
Mobile Country Code 2.15.3
Modification detection 2.12.17
Modification detection code 2.12.12
Monitoring events of information security of telecommunication network 2.14.19
Monitoring system of information security of telecommunication network 2.14.18
Moral and Ethical protection means 2.13.7
Multilevel device 2.13.6
Multilevel protection 2.10.7
Mutual suspicion 2.12.7
Need-to-know 2.9.43
Network access point 2.9.55
Network weaving 2.6.56
Non-repudiation 2.2.5
Notarization 2.12.16
Object 2.1.14
Object of information security of telecommunication network 2.14.22
Object of informatization 2.1.15
Objective of provision of information security of telecommunication network 2.14.36
Obstacle 2.10.9
Official secret 2.16.24
Offset track 2.18.10
One-way encryption 2.11.10
Open-security environment 2.10.8
Operator spoof 2.6.37
Organ of regime and secret 2.16.19
Organizational protection means 2.13.9
Padlocking 2.18.1
Passive attack 2.8.16
Passive treat 2.6.39
Passive wiretapping 2.6.40
Password 2.9.35
Penetration 2.6.53
Penetration testing 2.12.28

Personal Identification Number 2.15.5
Personal Unblocking Key 2.15.6
Phreaker 2.14.29
Physical access control 2.9.60
Physical protection 2.13.21
Physical protection means. 2.13.22
Physical threat 2.6.71
Piggyback entry 2.6.75
PIN 2.15.5
Plaintext 2.11.12
Policy of information security of telecommunication network 2.14.24
Privacy 2.1.18
Privacy protection 2.12.9
Private key 2.11.9
Procedural security 2.1.1
Procedural fraud 2.6.55
Program virus 2.6.51
Protectable rooms 2.16.8
Protected facility of computing machinery 2.1.4
Protected technical facility of informatization 2.1.5
Protected telecommunication network 2.14.7
Protection criterions of computer-based system 2.3.5
Protection criterions of facility of computing machinery 2.3.5
Protection facilities from unauthorized access 2.13.12
Protection from unauthorized access 2.10.3
Protection model 2.3.4
Protection of data 2.5.3
Protection of information 2.5.3
Protection of information from unauthorized access 2.5.4
Protection of information from unauthorized access 2.5.4
Protection of information sphere of telecommunication network 2.14.8
Protection profile 2.3.7
Protection strategy 2.3.8
Protection system of information from unauthorized access 2.4.5
Public key 2.11.11
Public-key cryptography 2.11.1
Quality of service of information security of telecommunication network 2.14.14
Quality of service of telecommunication network in condition of possible action of intruder 2.14.13
Read access 2.9.15
Read access control 2.9.41
Recovery plan 2.17.8

O'ZSTANDART
STANDARTLASHTIRISH
MAGRATINI
AXBOROT
JORIY ETISH

Reference monitor 2.9.10
Reference monitor concept 2.9.24
Regulation 2.10.12
Reliability 2.2.2
Removable User Identity Module 2.15.7
Replay attack 2.8.11
Repudiation 2.12.15
Residual data 2.12.19
Residual information 2.1.16
Residual risk 2.7.7
Risk 2.7.12
Risk acceptance 2.7.10
Risk analysis 2.7.1
Risk assessment 2.7.6
Risk criteria 2.7.4
Risk evaluation 2.7.8
Risk identification 2.7.3
Risk management 2.7.13
Risk management process 2.7.11
Risk of information security of telecommunication network . 2.14.25
Risk treatment 2.7.5
Sanitizing 2.12.22
Screening 2.10.15
Secrecy mode 2.16.18
Secret key 2.11.15
Secret information 2.16.23
Secret information leaking 2.16.26
Secret objects 2.16.20
Secret work 2.16.22
Sector alignment 2.18.2
Security 2.1.2
Security administrator 2.4.1
Security audit 2.4.3
Security category 2.5.6
Security class of computer-based system 2.3.3
Security class of facility of computing machinery 2.3.3
Security clearance 2.9.22
Security domain 2.10.1
Security filter 2.12.29
Security kernel 2.9.10
Security level 2.3.9
Security of data 2.5.1
Security of telecommunication network 2.14.4
Security of information 2.5.1

Security policy 2.3.6
Security policy realization 2.9.50
Security policy violator model 2.9.30
Security policy violator 2.9.31
Security policy. 2.9.39
Security system administration 2.4.2
Security target 2.3.2
Security tool 2.12.27
Security zone 2.10.4
Sensitive information 2.5.9
Sensitivity 2.5.10
Separation of duties 2.12.25
Service of information security 2.4.8
Service of information security of telecommunication network 2.14.27
Shell site 2.17.5
SIM-card 2.15.4
Single-level device 2.13.8
Social engineering 2.6.63
Soft token 2.9.44
Software bug 2.6.49
Software piracy 2.6.50
Spamming 2.6.59
Spiral track 2.18.11
Spoofing 2.8.17
Stability of functioning of telecommunication network 2.14.33
State secret 2.16.2
State secrets 2.16.3
Subject 2.1.22
Subject of information security of telecommunication network 2.14.28
Subject privilege 2.9.58
Subscriber Identification Module 2.15.4
Substitution 2.11.14
Supersector 2.18.12
Symmetric cryptography 2.11.16
System integrity 2.2.8
System of information security of telecommunication network 2.14.26
TCB 2.13.4
Technical facilities of informatization 2.1.23
Technical protection means 2.13.20
Technical protection of information 2.10.14
Technological security of telecommunication network 2.14.30

Terminal identification 2.9.20
Threat 2.6.65
Threat analysis 2.6.5
Threat model 2.6.30
Threat of information security of telecommunication network 2.14.31
Ticket 2.9.26
Time bomb 2.6.12
To tailgate 2.6.72
Top secret information 2.16.25
Trade secret 2.16.9
Traffic analysis 2.6.4
Traffic padding 2.6.45
Transposition 2.11.13
Trapdoor 2.6.28
Trojan 2.6.64
Trusted computer system 2.1.3
Trusted computing base 2.13.4
Unauthorized access 2.6.36
Unauthorized access to information 2.9.32
Unauthorized access to secret information 2.16.11
Unauthorized access to telecommunication network 2.14.21
Unauthorized action 2.6.35
Undocumented features 2.8.14
Universal Subscriber Identification Module 2.15.8
User identifier 2.9.18
User profile 2.9.45
User registration 2.9.48
Validation 2.12.5
Validation of objects of informatization 2.3.1
Verification 2.12.6
Violator 2.1.6
Virus 2.6.51
Virus signature 2.12.26
Vulnerability 2.6.68
Vulnerability of information 2.6.69
Vulnerability of telecommunication network 2.14.34
Weak bit 2.18.9
Wide track 2.18.13
Wiretapping 2.6.42
Worm 2.6.73
Write access 2.9.14
Write access control 2.9.40

STANDARTINFORM
NAZORATINI
AKSESIJT
JORIY ETISH

УДК 621.391 ОКС 01.040.35 Э 00

Ключевые слова: аутентификация, идентификатор, информационная безопасность, защита информации, целостность, доступность, конфиденциальность, несанкционированный доступ к информации, сети телекоммуникаций

O‘z DSt 2027 :2015

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

Начальник
научно-исследовательского отдела
криптографии О.Ахмедова

Ведущий инженер С.Абрамова

Младший научный сотрудник
научно-исследовательского отдела
криптографии Д.Джаматова

Нормоконтроль Л.Шаймарданова
23.12.2014

СОГЛАСОВАНО

Заместитель председателя
Государственного комитета связи,
информатизации и
телекоммуникационных
технологий Республики Узбекистан

М.Сангилов
письмо от 17.10.2014
№ 14-8/6173

СОГЛАСОВАНО

Служба национальной безопасности
Республики Узбекистан

письмо от 15.12.2014
№ 33/14481

СОГЛАСОВАНО

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

Ф.Умарходжаев
письмо от 03.10.2014
№ 32-13/1257